

**BY ORDER OF THE  
SECRETARY OF THE AIR FORCE**

**AIR FORCE MANUAL 14-304**

**23 DECEMBER 2016**



***Intelligence***

***THE SECURITY, USE, AND  
DISSEMINATION OF SENSITIVE  
COMPARTMENTED INFORMATION  
(SCI)***

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** This publication is available on the e-Publishing website at [www.e-publishing.af.mil](http://www.e-publishing.af.mil) for downloading.

**RELEASABILITY:** There are no restrictions on this publication.

---

OPR: AF/A2ZS

Certified by: AF/A2Z  
(Joseph D. Yount, SES)

Supersedes: AFI 14-302, 18 January 1994;  
AFI 14-303, 1 April 1999; AFMAN 14-304,  
1 May 1999; AFVA14-305, 1 April 2000;  
AFVA14-306, 1 April 2000; and AFVA14-  
307, 1 April 2000

---

Pages: 90

This publication implements Air Force Policy Directive (AFPD) 14-3, *Control, Protection, and Dissemination of Intelligence Information* and is consistent with Department of Defense Manual (DoDM) 5105.21, Volume 1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security*, DoDM 5105.21, Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security*, DoDM 5105.21, Volume 3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security and Special Activities*, and Intelligence Community Directive (ICD) 705, *Sensitive Compartmented Information Facilities*. It provides guidance on classification level, compartmentation, de-compartmentation, sanitization, release to foreign governments, emergency use, and additional security policy and procedures for the protection of intelligence information controlled as Sensitive Compartmented Information (SCI). It applies to the regular component, Air Force Reserve (AFR), Air National Guard (ANG), Department of the Air Force (DAF) Civilians, Government-Owned, Contractor-Operated and Contractor-Owned, Contractor-Operated facilities when required by contractual agreement. This publication requires the collection or maintenance of information protected by the Privacy Act of 1974. The authority to maintain the records prescribed in this publication are Title 10 U.S.C. 8013, *Secretary of the Air Force*; Air Force Instruction (AFI) 36-2608, *Military*

*Personnel Records System* and Executive Order 9397, *Numbering System for Federal Accounts Relating To Individual Persons*, as amended by Executive Order 13478, *Amendments to Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons*. The applicable Privacy Act System of Records Notices F031 497IG A, *Sensitive Compartmented Information (SCI) Personnel Records (June 11 1997, 62FR 31793)* is available. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW the Air Force Records Disposition Schedule located in the Air Force Records Information Management System. Air Force (AF) publications that authorize collecting information internal or external to the AF comply with the guidance provided in AFI 33-324, *The Air Force Information Collections and Reports Management Program*, which implements the Paperwork Reduction Act of 1995. Submit change recommendations using an AF Form 847, *Recommendation for Change of Publication* to the Office of Primary Responsibility (OPR). This publication may be supplemented, but all supplements are coordinated with the OPR prior to certification and approval. IAW AFI 33-360, *Publication and Forms Management*, the authorities to waive wing/unit level requirements in this publication are identified with a Tier (“T-0, T-1, T-2, T-3”) number following the compliance statement. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the AF.

### **SUMMARY OF CHANGES**

This publication has been revised and should be completely reviewed. The major changes include: updated guidance on classification level, compartmentation, de-compartmentation, sanitization, release to foreign governments, emergency use, and additional security guidance and procedures for the protection of intelligence information that is controlled as SCI. It clarifies the roles and responsibilities and incorporates organizational changes. It also includes guidance for the use of cellular telephone detectors in AF controlled SCI facilities, portable electronic devices (PED) and the requirement to report certain employment by former members accessed to SCI.

<b>Chapter 1— PROGRAM OVERVIEW AND OTHER COMPLIANCE AREAS</b>	<b>7</b>
1.1. Overview.....	7
1.2. SCI Security Management Program. ....	7
1.3. Special Security Office (SSO) System. ....	7
<b>CHAPTER 2— ROLES AND RESPONSIBILITIES</b>	<b>8</b>
2.1. Deputy Chief of Staff (DCS) for Intelligence, Surveillance, and Reconnaissance (ISR) (AF/A2).....	8
2.2. Air Force Cognizant Security Authority (AF CSA). ....	8

	2.3.	Director, Department of Defense (DoD) Consolidated Adjudication Facility (DoD CAF) .....	8
	2.4.	Commanders .....	8
	2.5.	Senior Intelligence Officer (SIO).....	8
	2.6.	Special Security Officer (SSO).....	9
Figure	2.1.	Request to Establish a New SSO. ....	11
Table	2.1.	MAJCOM SSOs. ....	12
	2.7.	Contractor Special Security Officer (CSSO).....	13
	2.8.	Special Security Representative (SSR)/Contractor Special Security Representative (CSSR).....	13
Figure	2.2.	SSR Appointment Letter.....	13
	2.9.	Director, Base Medical Service .....	14
	2.10.	Defense Force Commander.....	14
	2.11.	Base Civil Engineer. ....	15
	2.12.	Supporting Communications Element .....	15
	2.13.	Contractor Personnel Assigned to SSO. ....	15
	2.14.	Contract Personnel (not assigned to the SSO).....	16
<b>CHAPTER 3— PERSONNEL SECURITY AND ACCESS MANAGEMENT</b>			<b>17</b>
	3.1.	Chapter Overview. ....	17
	3.2.	Joint Personnel Adjudication System (JPAS).....	17
	3.3.	Scattered Castles.....	17
	3.4.	Department of Defense (DD) Form 1847-1,.....	17
	3.5.	Standard Form (SF) 312, .....	18
	3.6.	Indoctrination to SCI .....	18
	3.7.	Access to HCS, with Interim SCI Eligibility.....	20
	3.8.	KLONDIKE Control Systems (KCS).....	20
	3.9.	Special Circumstances .....	20
	3.10.	Reporting Derogatory Information. ....	24
	3.11.	Unauthorized Absences. ....	24

	3.12.	Missing Personnel.....	25
	3.13.	Incident Reports.....	25
	3.14.	Appeals Process/Due Process.....	25
	3.15.	Personal Status Changes.....	25
Figure 3.1.		Personal Financial Statement.....	26
Figure 3.2.		Intent to Marry or Cohabitate with a Non-US Citizen.....	28
	3.16.	Travel.....	28
	3.17.	Transfer-In-Status (TIS).....	29
<b>CHAPTER 4— INFORMATION SECURITY</b>			<b>30</b>
	4.1.	Chapter Overview.....	30
	4.2.	HUMINT Control System (HCS) Information.....	30
	4.3.	Originator Controlled (ORCON) Information.....	30
	4.4.	North Atlantic Treaty Organization (NATO) Classified on JWICS Systems.....	30
	4.5.	Security Review Process (Pre-Publication Review).....	31
	4.6.	Marking Classified Documents.....	31
	4.7.	Classified Coversheets.....	32
	4.8.	DIA CAB.....	32
<b>CHAPTER 5— SECURITY INCIDENTS</b>			<b>33</b>
	5.1.	Overview.....	33
	5.2.	Initial Reporting.....	33
Figure 5.1.		Initial Report of Security Incidents.....	33
Figure 5.2.		Assignment of Security Incident Number.....	35
	5.3.	Final Report.....	35
Figure 5.3.		Final Security Incident Report.....	36
<b>CHAPTER 6— PHYSICAL SECURITY</b>			<b>37</b>
	6.1.	Overview.....	37
	6.2.	Sensitive Compartmented Information Facilities (SCIFs).....	37
	6.3.	Co-Utilization of SCIFs.....	37
	6.4.	Special Access Programs (SAPs) Within DIA Accredited SCIFs.....	37

Figure 6.1.	SAP CUA Request.....	37
6.5.	SCIF Entry and Exit Inspections.....	38
Figure 6.2.	Furniture and Equipment Log.....	39
Figure 6.3.	Prohibited Electronic Equipment.....	40
Figure 6.4.	Facility Authorization Letter.....	43
Figure 6.5.	User Agreement for Personal Portable Electronic Devices (PED).....	44
Figure 6.6.	Device Prohibited Capabilities or Characteristics.....	46
Figure 6.7.	PED Prohibited Capabilities Matrix.....	48
6.6.	SCIF Accreditations and Inspections.....	51
Figure 6.8.	Concept Approval.....	51
6.7.	Temporary Secure Working Areas (TSWA) and Temporary SCIFs (T-SCIF).....	52
Figure 6.9.	Temporary Secure Working Area (TSWA) Request.....	53
Figure 6.10.	TSWA Standalone Computer SOP.....	55
6.8.	Changes to Security Posture.....	56
6.9.	Transfer of Security Cognizance.....	56
6.10.	Alarm System/Penetration/Security Response Testing.....	56
Figure 6.11.	Alarm System and Guard Response Test Log.....	57
6.11.	Unclassified Speakerphones in a DIA Accredited SCIF.....	57
6.12.	Cellular Telephone Detectors.....	57
6.13.	VTC Systems.....	58
6.14.	Badging Programs.....	58
6.15.	Control of Compromising Emanations (TEMPEST).....	59
<b>CHAPTER 7— VISITOR CONTROL</b>		<b>61</b>
7.1.	Overview.....	61
7.2.	JPAS or Scattered Control.....	61
7.3.	Visits to Foreign-Owned Facilities.....	62
7.4.	Visits By Foreign Nationals.....	62
7.5.	Escorts.....	62
7.6.	Contractor Special Security Officers (CSSO).....	62

<b>CHAPTER 8— INDUSTRIAL SECURITY</b>	<b>63</b>
8.1. Overview.....	63
8.2. Facility Security Clearance (FCL) Requirements for Access to SCI.....	63
8.3. Contractor/Consultant Security.....	63
Figure 8.1. DD Form 254 SCI Addendum. ....	63
8.4. DD Form 254 Preparation.....	64
8.5. Subcontractors. ....	65
8.6. Contracts Affecting other MAJCOMs/Bases.....	65
8.7. Contractor Visit Authorizations.....	65
8.8. SSO Record Keeping Requirements for Contractors.....	66
8.9. Release of Intelligence to US Contractors. ....	66
8.10. Foreign Ownership, Control, or Influence (FOCI). ....	67
Figure 8.2. National Interest Determination Request.....	68
<b>CHAPTER 9— SECURITY EDUCATION TRAINING AND AWARENESS PROGRAM (SETA)</b>	<b>70</b>
9.1. Overview.....	70
9.2. SCI Security Education Program. ....	70
9.3. Education and Training Responsibilities. ....	70
<b>Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b>	<b>72</b>
<b>Attachment 2— SCI SCREENING INTERVIEW</b>	<b>87</b>
<b>Attachment 3— CERTAIN POST-GOVERNMENT EMPLOYMENT BY HOLDERS OF SCI ACCESS</b>	<b>90</b>

## Chapter 1

### PROGRAM OVERVIEW AND OTHER COMPLIANCE AREAS

**1.1. Overview.** This publication provides guidance and procedures for security, use, and dissemination of SCI and collateral intelligence. It details the process for classification, compartmentation, de-compartmentation, sanitization, release of SCI to foreign governments, emergency use, and details additional security policies.

**1.2. SCI Security Management Program.** Provides the AF an exclusive, responsive, and secure means to receive, store, send, use, destroy, and protect SCI. The program assists individuals working with SCI material by providing instructions to avoid compromise and ensure its dissemination to appropriate users. It also protects SCI information from interference by un-cleared and unauthorized personnel and means.

**1.3. Special Security Office (SSO) System.** Protects sources and methods by providing critical support to intelligence operations with SCI security expertise and actions in the areas of physical, personnel, information, industrial and information system security.

## CHAPTER 2

### ROLES AND RESPONSIBILITIES

**2.1. Deputy Chief of Staff (DCS) for Intelligence, Surveillance, and Reconnaissance (ISR) (AF/A2).** IAW HAF Mission Directive 1-33, *Deputy Chief of Staff of the Air Force, Intelligence, Surveillance & Reconnaissance*, AF/A2 is the Head of the Intelligence Community Element (AF HICE) and the Senior ranking Intelligence Officer for the Headquarter Air Force/Secretary of the Air Force Staff. The AF/A2 is responsible for intelligence information security for the AF and has authority for all actions regarding the security, use, and dissemination of SCI.

**2.2. Air Force Cognizant Security Authority (AF CSA).** AF Special Security Management Division Chief (AF/A2ZS) is the AF CSA. The AF CSA:

2.2.1. Is the approving authority for all security related issues and has the authority to direct and implement SCI security guidance and procedures. **Note:** The Defense Intelligence Agency (DIA) is the Accrediting Official for physical and TEMPEST matters within DIA-accredited Sensitive Compartmented Information Facilities (SCIFs). The National Security Agency (NSA) is the CSA for physical, TEMPEST, and IS matters within NSA-accredited SCIFs.

2.2.2. Represents the AF/A2 on public disclosure and declaration issues.

2.2.3. Is the Scattered Castles access manager, approving authority, and the Scattered Castles Executive Steering Group (SCESG) representative for the AF.

2.2.4. Is the Joint Personnel Adjudication System (JPAS) manager for establishing the "Parent and Affiliated" user roles for the AF.

2.2.5. Is the AF representative on the National Security Agency (NSA) Access Control Working Group (ACWG) and has authority over all systems linked to the Intelligence Community Badge System (ICBS) and the Intelligence Community Badge Interoperability Program (ICBIP).

**2.3. Director, Department of Defense (DoD) Consolidated Adjudication Facility (DoD CAF).** The Director, DoD CAF, under the authority, direction, and control of the Director of Administration and Management (DA&M) adjudicates security clearance eligibility determinations, trustworthiness, and special access determinations, including SCI eligibility for all regular component, AFR, ANG, civilian and contractor personnel for the Department of the Army, Department of the Navy, DAF, Joint Chiefs of Staff, industrial contractor employees who fall under the National Industrial Security Program (NISP), and DoD Agencies.

**2.4. Commanders.** Suspend access to SCI when information exists raising a serious question as to the individual's ability or intent to protect classified information, provided that the commander follows procedures in DoD 5200.2-R, paragraph C8.1.3. Consult with your servicing legal office for advice on disciplinary issues for military member, labor law issues for civilian employees, and contract issues for contractors.

**2.5. Senior Intelligence Officer (SIO).** The SIO is defined as the Airman responsible for intelligence functions and operations within an organization. Unless otherwise directed by the

Wing Commander, this is the highest-ranking AF Airman within the organization that has: 1) been awarded an AF intelligence Specialty Code or civilian occupational series and 2) is serving in an AF intelligence position. This position is synonymous with the Chief of Wing Intelligence (CWI), where applicable. SIOs may delegate, except where specifically prohibited, the authority to discharge SIO responsibilities required by this instruction or other SCI security directives. The SIO is also responsible for the management of intelligence systems under their purview. In addition to the responsibilities outlined in DoDM 5105.21-V1, SIOs will:

2.5.1. Align the SSO directly under the SIO to effectively execute the full range of SCI security responsibilities assigned to the office (T-2).

2.5.2. Ensure commanders comply with responsibilities in Paragraph 2.19 through 2.21, and report all personnel data pertaining to SCI-indoctrinated individuals to the DoD CAF through their SSO, as required by this manual and AFI 31-501, *Personnel Security Program Management* (T-2).

2.5.3. Maintain the integrity of the SCI control system and ensure SSO personnel do not perform duties or details conflicting or interfering with their SCI security responsibilities or with security of SCI. Assigned SSO personnel should not perform duties as the unit collateral Security Manager (SM). SM duties could conflict or interfere with SSO personnel's SCI duties and responsibilities. Assigned SSO personnel should not perform duties as SSRs for other units or any other duties that might be a conflict of interest with their SSO duties (T-2).

2.5.4. Act as the local access approval authority for SCI material for personnel, including contractors, AFR, and ANG members (T-2).

2.5.5. Initiate a Memorandum of Agreement (MOA) with the supporting communications element to support dedicated intelligence systems and to provide timely communications support (T-2).

2.5.6. Approve, in writing, contractors that are authorized to access and secure a SCIF (T-1). The approval is conditional on the SCIF being the primary place of performance and security procedures being in-place to safeguard Caution-Proprietary Information Involved (PROPIN), Originator Controlled (ORCON), and other special program category (SPECAT) information. This duty can be delegated to the SSO.

**2.6. Special Security Officer (SSO).** SSOs are directly responsible to and functionally subordinate to the SIO.

2.6.1. Major Command (MAJCOM) SSO. The MAJCOM SSO manages the SCI security program for the MAJCOM, DRU, or FOA and oversees SCI security functions for subordinate SSOs and SCIFs. For the purposes of this instruction, the SSOs listed in Table 2.1 are considered MAJCOM SSOs. MAJCOM SSO will:

2.6.1.1. Establish a command-wide viable SCI security program and ensure each SCI Facility (SCIF) is accredited/reaccredited IAW ICD 705, *Sensitive Compartmented Information Facilities* (T-0).

2.6.1.2. Establish a working relationship with the tenant IC organization(s) located on the installation (T-1).

2.6.1.3. Establish a command-wide SSR/CSSR training program (T-1). The training responsibility may be delegated to the unit SIO or SSR. Training is documented and records kept as long as the individual holds the position in the assigned organization.

2.6.1.4. Establish a command-wide COR security responsibilities training program if they have oversight of contractors and contracts requiring a DD Form 254, *Department of Defense Contract Security Classification Specification* (T-1). The training responsibility may be delegated to the unit SIO or SSR. Training is documented and records are kept as long as the individual holds the position as described on the current contract.

2.6.1.5. Provide SCI security policy interpretation and implementation to subordinate organizations ensuring the policies do not conflict with Host Base procedures (T-1).

2.6.1.6. Review the MAJCOM Compartmented Address Book (CAB) account entries and submit any updates as necessary (T-2).

2.6.1.7. Establish and approve below the MAJCOM SSOs (T-1). The approving SIO appoints the SSO and various SCI compartment control officers and provides CAB data on the newly established SSO to the CSA within 30 days of establishment.

**Figure 2.1. Request to Establish a New SSO.**

<b>SAMPLE REQUEST FOR APPROVAL TO ESTABLISH A NEW SSO</b>
<p>FROM: (Requesting Unit)            TO: MAJCOM SSO/SIO (To AF CSA if establishing a MAJCOM SSO)            INFO: AF CSA            SUBJECT: Request to Establish a Special Security Office at _____.</p> <ol style="list-style-type: none"> <li>1. Request approval to establish an SSO at <u>(Unit and Location)</u>.</li> <li>2. The SIO will be:               <ol style="list-style-type: none"> <li>a. <u>(Rank and Name)</u></li> <li>b. <u>(Unit and Office Symbol)</u></li> <li>c. <u>(Duty Title)</u></li> </ol> </li> <li>3. Describe the Intelligence mission(s) the SSO will support and identify (by percentage of the unit's intelligence budget) the programs which fund that mission (e.g. 10% is National Intelligence Mission [NIP funded] and 90% is funded Military Intelligence Mission [MIP]).</li> <li>4. Indicated operating location of the SSO (along with SCIF ID number) (<b>DON'T include accreditation information</b>). Will bed down of the SSO require building a new SCIF or expanding an existing one?</li> <li>5. If an SSO already exists on the installation, explain why it cannot provide or continue to provide needed support.</li> <li>6. Will the SSO oversee subordinate SSOs and/or SSRs/CSSOs/CSSRs? If so, how many and where they are located? How many SCIFs will it support, both locally and geographically separated?</li> <li>7. How many people will it directly support locally; indirectly at Geographically Separated Units?</li> <li>8. Does the organization have a Defense Special Security Communications System (DSSCS) Routing Indicator ("Y" Route) and Plain Language Address (PLA)? If so, what is the PLA?</li> <li>9. What kind of SCI communications information systems support the organization? How many workstations?</li> <li>10. Who is/will be the DoDIIS Site Information Systems Officer/Manager (ISSO/ISSM)?</li> <li>11. If the organization is already a part of another unit's DoDIIS Site, supported by their ISSO/ISSM, will the organization continue to operate under that site or establish a new site?</li> <li>12. How many people, and at what pay grades, will be assigned to the SSO? It must be the primary duty of all personnel assigned to the SSO, and they must be trained in SSO duties. Broad security knowledge and familiarity with the intelligence community are required.</li> <li>13. Include any additional information you believe supports the requirement for an SSO.</li> <li>14. POC is <u>(Name/Rank/Contact Number)</u>.</li> </ol> <p>Signature Block</p>

2.6.1.8. Reports 'Insider Threat' information on a quarterly basis using the template and guidance located in the AF/A2ZS SharePoint site (T-1). The quarterly report is sent to

the AF CSA via JWICS by the established suspense dates: 1<sup>st</sup> Quarter 01 May, 2<sup>nd</sup> Quarter 01 Aug, 3<sup>rd</sup> Quarter 01 Nov, 4<sup>th</sup> Quarter 01 Feb.

2.6.1.9. Report statistical data on all security violations and infractions on a quarterly basis using the template and guidance located in the AF/A2ZS SharePoint site to the AF CSA (T-1). The quarterly report is sent to the AF CSA via JWICS by the established suspense dates: 1<sup>st</sup> Quarter 01 May, 2<sup>nd</sup> Quarter 01 Aug, 3<sup>rd</sup> Quarter 01 Nov, 4<sup>th</sup> Quarter 01 Feb. The report may be included in the Insider Threat Program report.

**Table 2.1. MAJCOM SSOs.**

<b>MAJCOM SSOs</b>		
<b>SSO</b>	<b>Location</b>	<b>Workflow Email</b>
SSO ACC	Joint Base Langley-Eustis, VA	ACCA2.A2S.ChiefSpecialSecurityOffice@us.af.mil
SSO AETC	Randolph AFB, TX	aetcsso@us.af.mil
SSO AFGSC	Barksdale AFB, LA	afgsc.a2s.workflow@barksdale.af.mil
SSO AFMC	Wright-Patterson AFB, OH	afmc.a2s.workflow@wpafb.af.mil
SSO AFOSI	Marine Corps Base Quantico, VA	afosi.hq.ipo@us.af.mil
SSO AFOTEC	Kirtland AFB, NM	afotecsso@kirtland.af.mil
SSO AFRC	Robins AFB, GA	afrc.sso@us.af.mil
SSO AFSOC	Hurlburt Field, FL	afsoc.a2s.wf@us.af.mil
SSO AFSPC	Peterson AFB, CO	a2s.wf@peterson.af.mil
SSO ANG	Joint Base Andrews, MD	angrc.a2-sso@ang.af.mil
SSO PACAF	Joint Base Pearl Harbor-Hickam, HI	pacaf.a2s@us.af.mil
SSO AFDW	Pentagon, Washington DC	usaf.pentagon.afdw-a2.mbx.afdw-a2s-af-sso--workflow@mail.mil
SSO USTRANSCOM (AMC)	Scott AFB, IL	transcom.scott.tcj2.mbx.sso@mail.mil
SSO USAFE	Ramstein AB, GE	usafea2.a2s.sso@us.af.mil
SAF/AAZ	Pentagon, Washington DC	usaf.pentagon.safaa.mbx.saf-aaz-workflow@mail.mil
SSO NASIC	Wright-Patterson AFB, OH	NASIC.SOORGBOX@us.af.mil

2.6.2. Unit SSO. Unit SSOs will:

2.6.2.1. Meet and comply with all requirements and responsibilities as outlined in DoDM 5105.21-V1 (T-0).

2.6.2.2. Ensure commanders report all personal data pertaining to SCI-indoctrinated individuals to the DoD CAF through their SSO, IAW this publication and AFI 31-501 (T-1).

2.6.2.3. Interact with multiple access databases (Joint Personnel Adjudication System [JPAS]/Scattered Castles) to validate/update security related information (T-2).

2.6.2.4. Conduct a reassessment of the need-to-know for all SCI positions in coordination with the SIO on an annual basis (T-2). The MAJCOM SSO compiles processes and sends to AF/A2ZS-CSA using RMT messaging or an official e-mail over JWICS.

2.6.3. Host base SSO responsibilities are not to cross command lines of authority with respect to management of resources (i.e. manpower and funding). Host base SSOs will assess the condition and security of systems supplied to the tenant (i.e. Cyber security, IDS, Access control) (T-1). MOAs are established to ensure host responsibilities (i.e. JWICS security controls) are met.

**2.7. Contractor Special Security Officer (CSSO).** CSSO will follow the responsibilities and training requirements IAW DoDM 5105.21-V1 (T-0).

**2.8. Special Security Representative (SSR)/Contractor Special Security Representative (CSSR).** DoDM 5105.21-V1 contains the duties and responsibilities of SSRs/CSSRs. The primary/alternate SSR/CSSR is nominated by the unit commander or SIO in writing, to the SSO, for each SCIF. (**Exception:** For overseas locations, the appointed SSR/CSSR requires 18 months remaining on station (except remote/deployed locations)). The SSR/CSSR will physically occupy the SCIF when operationally feasible (T-1).

**Figure 2.2. SSR Appointment Letter.**

<b>SAMPLE SSR APPOINTMENT LETTER</b>	
MEMORANDUM FOR MAJCOM SSO	
FROM: SSR's UNIT	
SUBJECT: Appointment of Special Security Representative (SSR)	
1. The below named individual(s) is/are appointed the SSR(s) for <u>unit</u> . The SSR will be responsible for complying with the duties and responsibilities as described in DoDM 5105.21-V1 and as designated by the <u>MAJCOM</u> Special Security Office.	
<b>Primary:</b>	
Rank/Name (Last, First MI)	Duty Phone:
<b>Alternate:</b>	
Rank/Name (Last, First MI)	Duty Phone:
2. This memorandum supersedes any previous appointment letter.	
3. If you have any questions please contact <u>POC</u> .	
<u>SIO Signature Block</u>	
<b>Note:</b> For contractor SSRs add a paragraph specifying if the appointed contractor SSR has been authorized to access/secure the SCIF.	

2.8.1. If a single SSR is appointed to multiple SCIFs, the commander/responsible SIO submits a request to the supporting SSO, outlining the rationale for a single SSR supporting more than one SCIF. All requests must:

2.8.1.1. Justify the need for the SSR to serve as the appointed security official for more than one SCIF (T-1).

2.8.1.2. Include cost and mission impacts if the waiver request is denied (T-1).

2.8.1.3. Indicate risk management measures that are established for handling SCI security management duties for multiple SCIFs on a daily basis (T-1).

2.8.1.4. Identify the SCIFs involved and their proximity to one another within the same building (T-1). Requests are only considered for SCIFs in the same building.

2.8.1.5. Staff the request through the supporting SSO and MAJCOM SSO, MAJCOM SIO is the final approval authority (T-1). MAJCOM SIO has discretion to delegate the approval authority to the MAJCOM SSO.

2.8.2. The appointed SSR does not perform SCI security duties for multiple SCIFs without the final approval of the MAJCOM SIO or delegated authority.

2.8.3. A single SSR supporting multiple SCIFs is considered a risk and requires annual review to ensure adherence to the SCI security program guidelines. During the annual review, if the program functions normally without incident, then the approval remains in effect until the next annual review. However, if security deviations are observed and determined to be a result of this management style, the MAJCOM SIO, through the MAJCOM SSO, makes a policy revocation determination regarding the continuation of approval. If required, revocations are issued in writing to the cognizant SIO/SSO and SSR. The MAJCOM SIO may withdraw their approval granting permission for a single SSR to support multiple SCIFs at any time.

2.8.4. SSRs maintain training documentation which reflects SCI security management training was completed. Documentation includes the SSRs certification showing contractors are qualified to perform SCI security functions within the SCIF.

**2.9. Director, Base Medical Service** . In the event an SCI-indoctrinated individual require, physical or psychological treatment potentially impacting their ability to perform sensitive duties, the Director of Base Medical Service formally notifies the unit commander of proposed treatment(s). Commanders coordinate with the SIO and SSO and make a determination whether to allow the person's continued access to sensitive information).

**2.10. Defense Force Commander.** The Defense Force Commander will:

2.10.1. Provide physical protection support for approved SCIFs IAW AFI 31-101, *Integrated Defense*, Intelligence Community Technical Specification (IC Tech Spec) *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.3* Intelligence Community Standard (ICS) 705-1, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities*, Intelligence Community Standard (ICS) 705-2, *Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information*, and this publication (T-0).

2.10.2. Coordinate with unit commanders and establish procedures for security teams to respond to point of alarm to determine if it is hostile or non-hostile. If hostile take appropriate actions to neutralize threats. If non-hostile then establish cordon and protect until the arrival of appropriately SCI cleared responder who assess the situation and provide guidance (T-1).

2.10.3. Allow the SIO, SSO, or designated representative access to the daily blotter to determine which entries may affect the continued eligibility of SCI-indoctrinated personnel or may affect the security of any SCIF area (T-1).

2.10.4. Assists owner/users in developing Protection Level Designation Matrix (PLDM) recommendations to the Installation Commander to assign appropriate protection levels and ensure it is protected IAW AFI 31-101 (T-1).

**2.11. Base Civil Engineer.** The Base Civil Engineer will:

2.11.1. Ensure all SCIF construction and/or modifications are coordinated with local CE and MAJCOM SSO prior to design requests; construction or modifications to facilities designated as SCIFs be IAW ICD 705 standards (T-0).

2.11.2. Handle requests for assistance on security-related problems in SCIFs on a priority basis (T-1).

2.11.3. Ensure the request for SCI-level shielded enclosure includes the following (T-0):

2.11.3.1. The Committee on National Security Systems Instruction (CNSSI) 7000, *TEMPEST Countermeasures for Facilities (C)* analysis.

2.11.3.2. The DIA/SEC Certified TEMPEST Technical Authority (CTTA) analysis.

2.11.3.3. A letter or message from local SIO or SCI security official stating the shielded enclosure is necessary to maintain security of the proposed SCIF.

**2.12. Supporting Communications Element .** The Supporting Communications Element will:

2.12.1. Operate and maintain dedicated intelligence communications systems to provide timely intelligence communications support (T-1).

2.12.2. Provide Communications-Electronics and COMSEC programming for communications according to the supported unit's validated requirements (T-1).

2.12.3. Appoint COMSEC officers and custodians (T-1).

2.12.4. Provide resources, on a rapid response basis, to meet the needs for communications service during peak activities, catastrophes, or fluctuations in the intelligence mission (T-1) These resources are established in the circuit restoration priority list or other authoritative source, such as a MAJCOM operations plan or local directive.

**2.13. Contractor Personnel Assigned to SSO.** Contractor personnel perform SCI personnel security support functions (preparing documents, scheduling, verifying information, giving the indoctrination/debriefing presentations, etc.) within a DoD SCIF only under the direct supervision of a government employee or military person. Contractor personnel in a SSO may perform all security duties as assigned by the SSO and outlined in the Performance of Work Statement (PWS). Contract personnel will NOT perform the following actions:

2.13.1. Approve an indoctrination, suspension, debriefing, nor sign as a person accepting same on behalf the U. S. Government (T-1).

2.13.2. Act in any capacity as the chief of personnel security or perform any industrial security functions within an SSO. Act in any capacity as the chief or primary physical security manager for the SCIF to include decisions for building standards or funding issues (T-1).

2.13.3. Accept a nondisclosure agreement (NdA) or nondisclosure statement (NdS) for the United States (US) Government (T-1).

2.13.4. Conduct SCI screening interviews (T-1).

**2.14. Contract Personnel (not assigned to the SSO).** Contract Personnel will:

2.14.1. Conduct SCI security functions within their assigned SCIF (T-1).

2.14.2. Satisfy their contractual requirements and failure to resolve disputes over duties/responsibilities will result in removal from SCI security responsibilities (T-1). Contractual obligations normally take precedence unless they conflict with security or safety rules. Conflicts are immediately resolved to the satisfaction of the SSR, CSSR, SSO, SIO and the Contracting Officer's Representative (COR).

## CHAPTER 3

### PERSONNEL SECURITY AND ACCESS MANAGEMENT

**3.1. Chapter Overview.** This chapter details processes for granting, managing, and revoking individual access to SCI material.

**3.2. Joint Personnel Adjudication System (JPAS).** JPAS is the DoD personnel security clearance and access database. MAJCOM SSOs follow the Parent and Affiliated user roles established by the AF CSA. MAJCOM SSO manages the organizational SCI access program through JPAS or successor systems of records (example: DISS) and as well as any locally created databases.

**3.3. Scattered Castles.** Due to special access requirements, not all IC Agencies use JPAS. The IC implemented a secure method to validate and certify the security clearances and accesses of its affiliated personnel. This method is necessary for providing additional secure and authenticated clearance verification for “Communities of Interest” (COI). A COI is a way to protect the need-to-know for specific information by limiting it to those individuals who have been previously approved to receive it. The result of this program is the establishment of the IC Security Clearance Repository (ICSCR), or more commonly referred to as Scattered Castles. The AF CSA is the Scattered Castles access manager, approving authority, and serves as the Scattered Castles Executive Steering Group (SCESG) representative for the AF.

3.3.1. MAJCOM SSOs or equivalent:

3.3.1.1. Nominate their subordinates for Scattered Castles access via JWICS e-mail to [A2ZS.workflow@af.ic.gov](mailto:A2ZS.workflow@af.ic.gov).

3.3.1.2. Maintain a list of their designated Scattered Castles users and notify AF CSA when a designated user no longer requires Scattered Castles access or is debriefed from SCI access.

3.3.2. The AF CSA starts the access approval process and contacts the nominee with the required information to complete the Scattered Castles access registration.

**3.4. Department of Defense (DD) Form 1847-1, *SCI Nondisclosure Statements (NDS)*.** During a member's initial SCI indoctrination the SSO uses the most current DD Form 1847-1 in addition to the federal statutes memorandum. As a condition of access to SCI, all AF personnel must sign DD Form 1847-1, *SCI Nondisclosure Statement (Nds)* that has a provision conforming to two Federal statutes: the Financial Services and General Government Appropriations Act (Public Law 112-74); and the Whistleblower Protection Enhancement Act (WPEA) (Public Law 112-199) (T-1).

3.4.1. The AF/A2 is responsible for retaining in a retrievable manner the original Nds for at least 70 years or until the death of the individual. The AF retains Nds records on AF military, civilians and contractor personnel.

3.4.2. It is AF and DoD policy to use the most current DD Form 1847-1 (NDS) attached with the Federal statutes for AF personnel the first time an individual is indoctrinated into SCI. The SSO completes the DD Form 1847-1 and updates JPAS. If JPAS reflects an NDS date there is no need to re-accomplish the NDS or enter a new date into JPAS.

3.4.2.1. All newly completed DD Form 1847-1 are scanned and maintained as the official AF record. Only new indoctrinations without an NdS on file (check JPAS) are sent to the servicing SSO's MAJCOM. The following steps are taken:

3.4.2.1.1. Scan both sides of DD Form 1847-1 (keep each record separate).

3.4.2.1.2. Use the following file naming convention: NDS\_MAJCOM\_YEAR\_LAST\_NAME\_FIRST NAME\_MIDDLE INTIAL (example: nds\_haf\_2014\_eason\_marcus\_a.pdf).

3.4.2.2. MAJCOM SSOs will send command's electronic NdS to the AF CSA for retention and nominate command's points of contact to AF CSA for access to the NdS SharePoint site (T-1).

3.4.2.3. The IC Form 4414 is used for the indoctrination into the HUMINT Control System (HCS) and available on the ODNI National Counter Intelligence Executive (NCIX) Security Executive Agent's (SECEA) website on NIPR Net at <http://www.ncix.gov/sea/index.php> (all lower case).

**3.5. Standard Form (SF) 312, *Nondisclosure Agreements (NdA)*.** All AF SCI security officials review collateral clearance levels, and NdA date in JPAS prior to performing SCI indoctrinations or requesting indoctrination assistance from other security officials. Individuals whose JPAS records do not reflect the required information are not indoctrinated until the collateral portion of their JPAS record is updated. JPAS is updated by the unit conducting the briefings. Refer to AFI 16-1404, *Air Force Information Security Program*, for NdA disposition instructions.

**3.6. Indoctrination to SCI .** Prior to SCI indoctrination the individual's eligibility is verified and a SCI Screening Interview, if required, is accomplished. Use a DD Form 1847 or IC Form 4414 to document SCI indoctrination.

3.6.1. Eligibility. SCI Security Officials use JPAS and/or Scattered Castles to determine if an individual is eligible for SCI indoctrination. The SIO may authorize indoctrination only after verification of eligibility and the need-to-know is established. Refer to ICD 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to SCI*, for detailed requirements regarding SCI eligibility.

3.6.1.1. SSOs accept SSBI, SSBI Periodic Reinvestigations (SSBI-PR) and Phased Periodic Reinvestigations (PPR) less than five years old as being "in-scope" and the basis for initial or continued access to SCI for visiting personnel. Upon reviewing an investigation more than five years old but less than seven years old, the receiving SSO will check JPAS to ensure an investigation is initiated and annotated in the record for the individual to remain "In-Scope." When the investigation is not annotated, the receiving SSO ensures that a periodic review is initiated by the owning organization. If an investigation has NOT been initiated the "in-scope" status does not apply and access is not granted.

3.6.1.2. An investigations over the seven year anniversary date are considered out of scope regardless of investigation status and access is not be granted. AF CSA may extend past the 7 year mark "in-scope" for instances where the open SSBI/PR has not

closed. The MAJCOM SSO justify the continued access to SCI in writing. AF CSA's approval memo will not exceed one year for visits.

3.6.1.3. MAJCOM SSOs have the authority to accept the current SCI status (read-in caveats) pending the start of an overdue investigation with the acceptance of risk after the review of a current SF86.

3.6.2. SCI Pre-Screening Interview. The nominated individual completes a private pre-screening interview covering the period since the completion of the last investigation (Single Scope Background Investigation (SSBI) or Periodic Reinvestigation (PR)) to assure they continued to meet the ICD 704 standards. SCI pre-screening interviews are accomplished in a private face-to-face setting and require the completion of the SCI pre-screening interview (Attachment 2). Interviewee provides a narrative explanation for all "yes" answers in the additional comments section of Attachment 2. If an interviewee declines to provide such information, interviewer documents this in the additional comments section. Failure to explain "yes" answers slow the adjudicative process, delay access, and could lead to the denial of access.

3.6.2.1. When the SCI screening results disclose information potentially disqualifying an individual from receiving access to SCI, at the commander's discretion a Security Information File (SIF) may be established IAW AFI 31-501.

3.6.2.2. Applicants have the option to withdraw from the screening process at any time but are not indoctrinated for SCI prior to adjudication.

3.6.3. Post-Government employment reporting. Post-Government employment reporting applies to individuals who occupy AF covered positions to report employment with foreign government entities (hereafter referred to as "covered employment") for two years after separation from the DAF.

3.6.3.1. Post-Government employment reporting requirements apply to positions associated to SCI accesses and implements Title 50 U.S.C. Section 3073a. SSOs provide Attachment 3, *Post-Government Employment by Holders of SCI Access*, to the appropriate employee during SCI in-brief and debrief. (Note: For purposes of this requirement all personnel assigned to 25th AF and its subordinate units, to include AFR units associated with 25th AF are assigned to an ISR organization.) AF Element of the IC ; consist of those Active Duty, AFR, ANG, and DAF Civilians employees who fit one or more of the following categories:

3.6.3.1.1. Awarded a 14N or 1N Air Force Specialty Code (AFSC) (military);

3.6.3.1.2. Assigned to a 0132 - job series (civilians);

3.6.3.1.3. Assigned to a Defense Civilian Intelligence Professional System (GG), Defense Intelligence Senior Executive Service (DISES), or Defense Intelligence Senior Leader (DISL) billet (civilians);

3.6.3.1.4. Assigned to an AF ISR organization, including appointees from other agencies (excluding Contractors);

3.6.3.1.5. Assigned to AFOSI.

3.6.3.2. The AF/A2 CSA consults with appropriate security and counterintelligence authorities to conduct a risk assessment and recommend mitigation upon receiving notice from any employee involving employment with a foreign government entity.

3.6.3.3. SSOs retain the signed form in the employee's Personnel Security Folder, and dispose of them IAW rule applying to the in-brief and debrief form. SSO provides a copy of the form to employee completing them on request.

3.6.3.4. An employee currently indoctrinated into SCI and in the position listed above, SSOs ensure the employee completes the form letter within 180 days (T-1).

**3.7. Access to HCS, with Interim SCI Eligibility.** All the SCI access requirements in ICD 704 and Intelligence Community Policy Guidance (ICPG) 704.1, *Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*, apply to HCS access.

3.7.1. Before an individual with interim SCI access is considered for indoctrination into HCS Programs the SSO ensures:

3.7.1.1. An open Single Scope Background Investigation (SSBI)

3.7.1.2. A favorable SCI Screening Interview; and be granted interim SCI access by the DoD CAF. **Exception:** Technical training students with interim SCI eligibility exempt from submission of the formal waiver requirement to access HCS.

3.7.1.3. When all conditions are met, the responsible security official through their MAJCOM SSO requests indoctrination approval from the AF CSA by email through the AF/A2ZS workflow email address ([usaf.pentagon.af.a2.mbx.af-A2ZS-workflow@mail.mil](mailto:usaf.pentagon.af.a2.mbx.af-A2ZS-workflow@mail.mil)). Access should be kept to a minimum, pending final clearance adjudication.

3.7.2. Indoctrinating interim SCI individuals into HCS may not automatically grant the individual access to all the IC databases needed. Certain IC database accesses are controlled by Scattered Castles and do not recognize interim SCI eligibility as a proper clearance. In this case, the SSO needs to contact the database point of contact (POC) to develop a workaround for individual access.

3.7.3. Document HCS indoctrination using forms DD Form 1847 or IC Form 4414. (**Exception:** When an owning organization requests indoctrination assist the accepting organization should follow the requesting organizations policies and use the form identified in the request.)

**3.8. KLONDIKE Control Systems (KCS).** All requests for KCS access, indoctrinations, and debriefings are channeled through the MAJCOM SSO. The MAJCOM SSO contacts AF CSA for detail instructions. KCS security incidents must be reported to AF CSA (T-0).

### **3.9. Special Circumstances**

3.9.1. Temporary/Interim Eligibility for Access to SCI. Temporary eligibility is needed when a commander has determined there is a justified requirement for access to SCI and an individual does not have the required investigation (SSBI) completed and favorably adjudicated. Temporary eligibility may be considered when the individual has a favorable *National Agency Check/National Agency Check plus Written Inquiries and credit check plus*

*Single Scope Background Investigation Requested along with an open SSBI that is running favorably (NACS).* If unfavorable information is discovered, temporary access is withdrawn. Individuals granted temporary eligibility is advised during the indoctrination their continued access is contingent upon favorable adjudication of the background investigation. A request for the temporary eligibility is forwarded through the MAJCOM SSO to the DoD CAF via JPAS. MAJCOM SSOs may delegate authority to their subordinates as necessary. The request indicates the individual's SF 86 was favorably reviewed by the requester. Conduct a pre-screening interview when temporary eligibility to SCI is required pending completion and adjudication of the SSBI. Attachment 2 contains an example of an SCI pre-screening interview. Temporary eligibility requests should be unclassified. Interim SCI requests are submitted through JPAS and the Clearance Adjudication Tracking System (CATS).

### 3.9.2. SCI Eligibility for Training Attendance.

3.9.2.1. Airmen selected for career/AFSC follow-on training or retraining into a new AFSC may require SCI eligibility as a prerequisite when applying for or prior to being assigned a class date. The Airman's current or losing local SSO and/or MAJCOM SSO processes the SCI eligibility request when this pre-requisite exists, regardless of the current AFSC, duty assignment or associated clearance requirements. When processing the request to the DoD CAF, the SSO and/or SIO cite the future training course or AFSC retraining selection as the justification criteria.

3.9.2.2. Airmen should not depart for training until JPAS reflects the required interim or final SCI eligibility by the DoD CAF. SCI indoctrination is not necessary prior to the individual's departure for the training location unless an indoctrination assist is requested by the training site SSO.

3.9.3. Access by Retired General/Flag Officers and Former Senior DoD Officials. The Secretary of the Air Force (SecAF), Chief of Staff of the Air Force (CSAF), MAJCOM commanders (MAJCOM/CC) or Headquarters AF two letter Directors may request the Administrative Assistant to the SecAF (SAF/AA) approve sponsorship for access to classified information for a retired general officer, Senior Executive Service (SES) member or former Presidential appointees to support a specific AF program or mission. Refer to AFI 31-501, for procedures to get clearance eligibility. After SAF/AA approves sponsorship, AF/A2 may grant SCI access to retired General/Flag Officers and former senior DoD officials in DoD-sponsored events when their expertise is vital.

3.9.3.1. Request is sent to the AF CSA and they approve the access unless there is disqualifying information. If there is disqualifying information, the AF CSA forwards the package to the AF/A2 for approval/disapproval.

3.9.3.2. The request includes the following information:

3.9.3.2.1. Visitor's Name.

3.9.3.2.2. Social Security Account Number (SSAN).

3.9.3.2.3. Sponsor's Name (General Officer or SES).

3.9.3.2.4. Date Access Required (maximum of one year).

3.9.3.2.5. Verification of ICD 704 standards (include any information potentially disqualifying).

3.9.3.2.6. Justification of “Need-to-Know”.

3.9.3.2.7. Statement stating visitor is not afforded any competitive advantage through material released to him/her.

3.9.3.2.8. Statement stating SAF/AA granted clearance eligibility on “DATE”.

3.9.4. Special Purpose Access (SPA). Individuals occasionally require access to SCI to perform a specific task. The local SIO may grant access, for consecutive periods of 180 days, not to exceed one year. The SPA is approved based on the criticality of the need-to-know and a favorable ICD 704 eligibility determination from the DoD CAF as entered in JPAS and/or Scattered Castles. Conduct a SCI screening interview (Attachment 2) to ensure no disqualifying information is present. Upon approval, the individual is to be given an indoctrination briefing which includes the basic information to protect SCI. The individual signs an NdS and is indoctrinated for the appropriate SCI access. Records of indoctrination for SPA include specific date of automatic debrief from SCI access. Extensions are requested and approved before automatic debrief date.

3.9.5. Intergovernmental Personnel Act (IPA) Employees. IPA employees are typically non-federal organization employees on temporary loan to the Federal Government for a specified period of time. IPAs requiring SCI access follow the same procedures for obtaining access as government employees. It is the responsibility of the IPA supervisor to initiate the security clearance/access process when an IPA requires SCI access for performing their duties outlined in the IPA Agreement.

3.9.5.1. The IPA Agreement. The IPA Agreement typically consists of an Optional Form (OF) 69, *Assignment Agreement*, with addendums addressing legal issues, costs, and other documentation required as part of the hiring process. If an IPA requires SCI access, the OF 69, (Part 7, Paragraph 22) states TS/SCI access is required for accomplishment of IPA duties. When requesting SCI access for an IPA, the following documents will be included with the IPA agreement (T-1):

3.9.5.1.1. The IPA SCI Addendum.

3.9.5.1.2. Justification for “SI/TK” access.

3.9.5.1.3. Justification for “G” access (if needed).

3.9.5.1.4. Justification for “HCS” access (if needed).

3.9.5.2. “Detailed” IPAs are the most common type employed by the AF within an SCI environment. Detailed IPAs are not government employees nor are they considered to be defense contractors. They are merely considered “IPAs” when described with that designation.

3.9.6. Scientific Advisory Board (SAB) SCI Access.

3.9.6.1. The SAB is a group of the nation’s top civilian scientists from industry, national labs, Federally Funded Research and Development Centers (FFRDCs), academia and government brought together to perform AF related studies at the behest of the Secretary of the Air Force (SecAF). All members are nominated by the SecAF, approved by the White House Liaison Office and appointed by the Secretary of Defense (SecDef) as

Special Government Employees (SGE). The SAB secretariat creates a civilian category in JPAS for all approved members.

3.9.6.2. Once sworn in as a SAB member SSO AFDW (AF District of Washington) receives SCI indoctrination request from the SAB secretariat for all members requiring SCI access. SSO AFDW:

3.9.6.2.1. Takes an owning relationship in JPAS with their SCI SMO (SSOAFDW2) under member's civilian category (if possible) and review JPAS and or scattered castles for eligibility determination.

3.9.6.2.2. If eligibility determination cannot be made (i.e., upgrade eligibility required) SSO AFDW requests a Request to Research/Upgrade (RRU) through JPAS to upgrade members eligibility level. Once eligibility is granted SSO AFDW either indoctrinates member or request indoctrination assistance to have members indoctrinated at location closest to where member resides. Once SSO AFDW receives indoctrination package JPAS civilian category is updated.

3.9.6.2.3. If a member already meets eligibility requirements, SSO AFDW approves the member for SCI indoctrination and, if required, submit indoctrination assistance to have the member indoctrinated at a location closest to where they reside.

3.9.6.2.4. If member is already indoctrinated into SCI access with another SSO as a civilian or contractor SSO AFDW makes every attempt to obtain a copy of indoctrination paperwork to hold in order to support SAB efforts. If currently indoctrinated as a civilian SSO AFDW takes a servicing relationship with member and pass SCI in support of SAB business only. If currently indoctrinated as a contractor, SCI accesses and JPAS ownership is to be placed in civilian category.

3.9.6.3. All regular component officers or reserve officers not permanently assigned to SAB secretariat but have been identified by the SAB as filling a temporary executive officers or technical writer's role are processed through SSO AFDW. SSO AFDW:

3.9.6.3.1. Verifies current eligibility status using JPAS or Scattered Castles.

3.9.6.3.2. Takes a servicing role in JPAS and permanently certify those accesses for support to SAB, if the regular component officers or reserve officer is already indoctrinated. If additional accesses are required, SSO AFDW contacts the owning SSO for permission to indoctrinate into additional accesses.

3.9.6.3.3. Receives a special purpose access request from the SAB secretariat on a regular component officer or reserve officer that are not already indoctrinated into SCI. Once DOD CAF approval is granted for SCI indoctrination, SSO AFDW either indoctrinates the member or process an indoctrination assistance to have member briefed at the local SSO. Once SSO AFDW receives the indoctrination package, the appropriate JPAS category is updated.

3.9.6.3.4. Administratively debriefs, no later than 15 Oct of each year, all regular component officer or reserve officers temporarily supporting the SAB. This applies only members owned by SSO AFDW. If ownership exists with another government SSO, SSO AFDW does not administratively debrief.

3.9.6.4. When contractors participate in the SAB as Subject Matter Experts (SME), the SSO holding their access permanently certifies the accesses to SSO AFDW with a request to recertify as required, not to exceed one year.

### **3.10. Reporting Derogatory Information.**

3.10.1. In addition to requiring self-reporting of information affecting SCI eligibility, SSOs/CSSOs maintain effective liaison with supervisory personnel, local police agencies, and, consistent with applicable health care laws and regulations, medical authorities to identify as early as possible potential security problems involving SCI-indoctrinated personnel. The DoD CAF retains authority to suspend an individual's eligibility based on information gained during adjudication or information reported by the field.

3.10.2. Security Information File (SIF). A SIF is a collection of documents established when derogatory information becomes known and may impact an individual's continued eligibility to hold SCI access and/or a security clearance. A SIF is established by a commander, a civilian equivalent, or the DoD CAF. Formal notification to the individual (in writing) is mandatory; once notification is complete the individual formally acknowledges (in writing) the SIF has been established. Once formally established, only the DoD CAF has closure authority. Refer to AFI 31-501, for SIF contents.

3.10.2.1. Military and Government Employees. If the SIF is locally established, the SSO notifies the DoD CAF, via approved channels; and the subject's parent MAJCOM SSO. If the SIF is DoD CAF established, the SSO notifies the subject's parent MAJCOM SSO.

3.10.2.2. Contractors/Consultants. If the SIF is locally established, the SSO notifies the DoD CAF, via approved channels; the MAJCOM SSO with security cognizance for the contract, the COR and the company Facility Security Officer (FSO). If the SIF is DoD CAF established, the SSO notifies the MAJCOM SSO with security cognizance for the contract, the COR and the company Facility Security Officer (FSO). (**Note:** Due to privacy restrictions, the FSO is informed only of the establishment of the SIF and, if applicable, suspension of access to classified information.) The FSO is advised to contact their employee for details regarding the incident.

### **3.11. Unauthorized Absences.**

3.11.1. Military Members. If a military member is not present for duty and currently has or has had access to TOP SECRET, SCI, or special access information then refer to AFI 36-2911, *Desertion and Unauthorized Absence*, for member disposition. If the military member is classified as a deserter IAW AFI 36-2911 immediately: establish a SIF; suspend the member's access to all classified information; and if the member had access to Special Access Programs (SAP) or programs utilizing Alternative or Compensatory Control Measures (ACCM) notify the appropriate program security official within 24 hours of the suspension.

3.11.2. Civilian and Contractor Personnel. For personnel with SCI access who are absence without authorization and lack of accountability of civilian or contractor personnel with SCI access for a 24-hour period (1 day); or have gone to/stayed in a foreign country, and while there, has asked for, or taken any type of asylum, or resident permit from that country, or its governmental agencies, should accomplish the following. Establish a SIF, suspend access to all classified information, and if the individual had access to SAPs or programs utilizing

ACCMs, notify the appropriate program security official within 24 hours of the suspension. For contractor personnel, notify both the COR and the company Facility Security Officer (FSO) of SIF establishment and all suspensions.

### **3.12. Missing Personnel.**

3.12.1. For all indoctrinated personnel killed, captured/missing in action, absent without leave, or considered a deserter the MAJCOM SSO will report to the AF CSA within 24 hours if personnel currently have or had SCI access within the last three years (T-1).

3.12.2. If an individual is reported missing, unit commanders notify their SSR to begin the process to check if that individual had SCI access within the last three years.

3.12.2.1. The unit Security Manager (SM) checks in JPAS to see if the subject is eligible for SCI access and if eligible, up-channel to the responsible SSO.

3.12.2.2. The responsible SSO verify SCI access, i.e., checking JPAS, Scattered Castles, calling prior unit, etc. If SCI access is verified, report the incident to the AF CSA within 24 hours. The report includes a summary of information the individual had access to and their full name, rank and SSN.

**3.13. Incident Reports.** Incident reports are completed and submitted via JPAS and Case Adjudication Tracking System (CATS). Submitting an incident report via JPAS and CATS automatically initiate a SIF if one was not already established. The DoD CAF is the only organization authorized to close a SIF or remove it from JPAS/CATS.

**3.14. Appeals Process/Due Process.** Procedures are contained in AFI 31-501. Due process packages for a contractor is be handled by the servicing SSO who coordinates with the COR before presenting the information to the individual and informing the FSO. **Note:** Due to privacy restrictions, the FSO is informed only that an appeal or due-process-action is initiated. The FSO is advised to contact their employee for details on these matters. The SSO consults with their servicing Staff Judge Advocate on the matter for additional guidance on minimizing AF or DoD liability. The subject forwards any rebuttal or appeal to the servicing SSO for forwarding to the DoD CAF. When a member elects to appeal DoD CAF clearance eligibility revocation, the SSO tracks the status of the appeal package. Thirty days after package is returned to the DoD CAF, SSO, thru the MAJCOM SSO and AF/A2ZS, requests confirmation that the package is in the possession of Defense Office of Hearings and Appeals (DOHA). The SSO advises the member and the respective commander once confirmation is received. PSAB/DOHA process may take 7 - 9 months for complete, depending on DOHA's workload and complexity of the individual cases. DOHA's decision is provided to the DoD CAF and placed in JPAS as the system of record.

**3.15. Personal Status Changes .** Administrative changes in status (e.g., name change, relocation, etc.) are not reported to the DoD CAF. SCI indoctrinated personnel will:

3.15.1. Provide advance written notification within 5 duty days to the servicing SSO when they who decided to marry or to cohabit with a foreign national and those who intend to enter into a relationship potentially creating a heightened risk of manipulation, blackmail, or coercion (T-1).

3.15.2. Provide written notification to the servicing SSO when they:

3.15.2.1. Change Marital Status or Cohabitation other than previously stated. (T-1).

3.15.2.2. Significantly change their financial status such as sudden affluence (receipt of \$10,000 or more from a source other than a pay raise/promotion) or financial distress (foreclosure or short sale of real estate, accounts sent to collection, repossessions, etc.). **Note:** A Personal Financial Statement (PFS) is completed in cases of financial distress. Refer to Figure 3.1, *Personal Financial Statement*. A commander or SSO may require a PFS if they have reason to believe an individual is experiencing financial problems to the extent eligibility for access to classified information may be called into question (T-0).

3.15.2.3. Experience other significant changes. Significant changes include, but are not limited to; arrest by any law enforcement agency; imposition of a restraining order or a “no contact” order by any civilian court; traffic violations which carry a fine/penalty of \$300 or more (not including court costs) or in which alcohol or drugs are involved even if not yet adjudicated. The commander may establish a SIF IAW AFI 31-501, when results disclose information potentially disqualifying an individual from receiving SCI access eligibility (T-1).

**Figure 3.1. Personal Financial Statement.**

<b>PERSONAL FINANCIAL STATEMENT (PFS)</b>	
CLASSIFICATION (AS REQUIRED, MINIMUM OF UNCLAS/FOUO)	
1.	Name, Rank or Grade, SSAN of person submitting statement.
2.	This statement is current as of <u>DATE</u> .
3.	Monthly Gross Income: <ol style="list-style-type: none"> <li>a. Salary (before deductions).</li> <li>b. Spouse’s income.</li> <li>c. Other income (include interest, dividends, etc.)</li> <li>d. Total income.</li> </ol>
4.	Monthly deductions (include deductions taken from spouse’s income): <ol style="list-style-type: none"> <li>a. Federal income tax (include any delinquent taxes).</li> <li>b. State income tax (include any delinquent taxes).</li> <li>c. Local tax (include any delinquent taxes).</li> <li>d. Social Security.</li> <li>e. Allotments.</li> <li>f. Other (specify what for and amount).</li> <li>g. Total Deductions.</li> </ol>
5.	Total monthly income, less deductions.
6.	Assets: <ol style="list-style-type: none"> <li>a. Real estate.</li> <li>b. Bank savings.</li> <li>c. Checking Account.</li> <li>d. Stocks, bonds, mutual funds, other investments.</li> <li>e. Personal assets (cars, furniture, etc.).</li> <li>f. Total assets.</li> </ol>
7.	Debts: <ol style="list-style-type: none"> <li>a. List all loans and charge accounts with name of person/company and purpose of loan</li> </ol>

(auto, furniture, home, etc.).

- b. Total owed on each loan/charge account and monthly payment.
- c. Total debts/payments.

8. Monthly expenses (Note: Omit any indebtedness which is being discharged by means of allotment as listed under para 4 deductions).

- a. Rent/mortgage.
- b. Total loan payment's: (From para 7c debits).
- c. Utilities (gas, electric, water, trash, telephone, etc.).
- d. Groceries.
- e. Clothing (to include dry cleaning and laundry).
- f. Car expenses (insurance, repairs, gasoline, oil, etc.).
- g. Insurance (life, medical, homeowners, property, etc.).
- h. Medical expenses (dental, medication, etc.).
- i. Alimony, child support, and child care expenses.
- j. Miscellaneous expenses (entertainment, sundries, etc.).
- k. Total monthly expenses.

9. Summary:

- a. Total monthly net income:
- b. Total monthly income:
- c. Remainder:

10. Remarks (include any additional data not specifically identified above which would have a bearing on the case).

**PRIVACY ACT STATEMENT FOR THE PERSONAL FINANCIAL STATEMENT**

**AUTHORITY:** Executive Order numbers 9397, 10450, 11905, 12065; Intelligence Community Directive 704.

**PURPOSE:** To enable member to submit a personal financial statement for Sensitive Compartmented Information (SCI) access adjudication. Used only by the SCI approval authority to assist in determining the member's eligibility for access to SCI.

**ROUTINE USES:** None

**DISCLOSURE IS VOLUNTARY:** Failure to provide the necessary information will result in the denial of SCI access eligibility

**Note:** If the commander makes a determination that a SIF is established due to financial consideration, the PFS should be part of the SIF package provided to the DoD CAF. (The SSO ensures a statement is added at the end of the PFS to indicate the individual has reviewed the PFS and certifies the data is correct prior to sending).

3.15.3. All written statements collected are forwarded by the SSO to the member's parent MAJCOM SSO/SIO to determine if the situation is likely to pose an unacceptable risk to national security. This determination is based on the value afforded to US Government national security interests by the individual having continued access to SCI exceeding the associated risks of the relationship. A record of the evaluation is kept locally. The evaluation includes such factors as:

3.15.3.1. The potential for a foreign power to exert influence over the intended spouse/cohabitant/roommate or immediate family members.

3.15.3.2. The possibility that ties to any foreign government exist.

3.15.3.3. Involvement in criminal activity.

3.15.3.4. Support for the overthrow of the US Government.

3.15.4. Based on the results of the evaluation the local commander and SIO determine if access suspension is warranted or if a Standard Form (SF) 86C, *Special Agreement Check*, is required.

3.15.5. Failure to provide proper notification requires initiation of a Security Information File including, but not limited to, all information shown in Figure 3.2, *Intent to Marry or Cohabitate with a Non-US Citizen*.

**Figure 3.2. Intent to Marry or Cohabitate with a Non-US Citizen.**

<b>INTENT TO MARRY OR COHABITATE WITH A NON-US CITIZEN NOTIFICATION</b>
CLASSIFICATION (as required, but a minimum of UNCLAS//FOUO)
FROM: LOCAL SSO
TO: MAJCOM/SSO
SUBJECT: (Rank, Name, SSAN) Intent to Marry/Cohabitate with a Foreign National
1. Statement of intent to marry/cohabitate: <ol style="list-style-type: none"> <li>a. Name, address, citizenship and vocation of intended spouse/co-habitant and his or her immediate family members.</li> <li>b. Nature and extent of contact subject has with the intended spouse/co-habitant's immediate family members.</li> <li>c. Political and vocational ties the intended spouse/co-habitant or his/her immediate family members have with his or her government.</li> <li>d. State whether or not individual is currently cohabitating with the intended spouse/cohabitant.</li> <li>e. Date SAC was initiated.</li> <li>f. Remarks (as required).</li> </ol>
2. Point of contact (POC) and telephone number.
<b>Note:</b> May be via Message or JWICS E-mail.

3.15.6. If required, the SSO has the member complete the Single Agency Check (SAC) and then route it through appropriate channels.

**3.16. Travel.** JPAS is the repository for unofficial foreign travel and SSOs ensure all unofficial foreign travel is added into JPAS. Each MAJCOM SSO establishes procedures for documenting official foreign travel for their MAJCOM, unless Intelligence Community Policy Memorandum 2007-700-3, *Director of National Intelligence Foreign Travel Reporting Form*, Paragraph D.3, applies. Any unusual incidents occurring during official or unofficial travel is reported to the Air Force Office of Special Investigations (AFOSI) through the local SSO within 72 hours of return.

**3.17. Transfer-In-Status (TIS).** TIS actions are authorized for operational necessities. It may be requested by either a losing or gaining SSO, however, the gaining SSO ultimately approve and accept the TIS action. **Exception:** Students attending Air Command and Staff College and Air War College automatically are TIS'd to SSO AU. All paperwork associated to the original indoctrination is made available to the gaining organization.

3.17.1. If requested, the losing SSO scans and electronically send the signed NdS to the gaining SSO.

3.17.2. Once the TIS is completed, the individual in-processes with the gaining SSO to receive the security awareness training.

## CHAPTER 4

### INFORMATION SECURITY

**4.1. Chapter Overview.** This chapter covers methods used to ensure access to Intelligence Community (IC) classification management and control markings system, which provides the framework for accessing, classifying, disseminating, and declassifying intelligence and intelligence-related information to protect sources, methods, activities. Refer to ICD 710, *Classification Management and Control Markings System*, for further guidance. For IC classification management and control markings system AF personnel follow the latest Intelligence Community Markings System Register and Manual.

**4.2. HUMINT Control System (HCS) Information.** HCS marking is marked HCS-P (Product) and HCS-O (Operations). In cases where the SIO determines mission requirements cannot be met using mail groups for dissemination of HCS, HCS e-mails may be sent desktop-to-desktop over appropriately authorized networks between HCS indoctrinated individuals within the AF and under the security cognizance of the AF HICE. It remains the sender's responsibility to verify the recipient of HCS information has been indoctrinated for HCS and has a need-to-know. E-mails containing HCS information is appropriately marked and the subject line indicates the e-mail contains HCS materials.

**4.3. Originator Controlled (ORCON) Information.** ORCON designated material disseminated to an AF headquarters may be released within the headquarters and further disseminated to subordinate units without advanced permission from the originating organization. This includes release to the recipient organization's contractors operating within a government facility. AF headquarters with staff elements and subordinate units with recurring requirements for ORCON information should notify the originating agency so these elements can be included as direct recipients of ORCON intelligence information. Refer to ICPG 710.1, *Application of Dissemination Controls: Originator Control (ORCON)*, for further guidance. ICPG 710.1, Sections D.9 and F.1.c.(1) is the standard criteria for IC ORCON Training. ORCON training addresses the proper use, application, safeguarding, process for dissemination, and derivative use of the ORCON marking.

**4.4. North Atlantic Treaty Organization (NATO) Classified on JWICS Systems.** SSO/Information System Security Manager (ISSM) ensures the following IAW DIA Installation Guide, *Approval Process For Handling NATO Classified on JWICS Subnets,* and AFI 16-1404.

4.4.1. As a minimum all JWICS users are briefed with the AF NATO Security Awareness Briefing and sign the AF NATO Security Awareness Acknowledgement prior to access onto JWICS. The NATO security awareness briefing and acknowledgement letter is used for individuals that require access to a classified system, but do not require daily access to NATO information. Acknowledgement letters are kept in the individuals Personnel Security File as long as the individual has access to JWICS. Both the briefing and acknowledgement letter can be found on the AF Portal: SAF/AAZ, AF NATO Security Awareness page.

4.4.2. JWICS systems and subnets required to handle NATO classified are authorized by the AO to process NATO classified information. The authorization memo states NATO Secret is approved to be processed on the system/network.

4.4.3. All JWICS systems authorized to process NATO classified information are properly marked. Consult the DIA Instruction Guide, “*Approval Process for Handling NATO Classified Information on JWICS Subnets*, Paragraph 2 or the local SSO for proper marking.

4.4.4. Refer to AFI 31-406 for storage, protection and transmission and report incidents involving NATO classified information on JWICS.

4.4.5. Information Protection Offices are the primary office of responsibility for NATO briefings. SSOs only brief personnel into NATO information awareness for JWICS users when the local IP requests the assistance.

4.4.6. Contractor access to NATO information is permitted. All contractors that have access to JWICS are briefed with the AF NATO Security Awareness Briefing and sign the security awareness acknowledgement. Granting NATO access does not require changes to the Statement of Work (SOW) due to access being in the interest of the US Government. DD Form 254 is completed to reflect access to NATO information.

**4.5. Security Review Process (Pre-Publication Review).** All military, civilian and contractor SCI-indoctrinated personnel submit for a pre-publication. (**Note:** This includes any material intended for disclosure that potentially contains SCI or SCI-derived information; proposed public statements on information derived from SCI or concerning SCI operations, sources, or methods; and; resumes or applications for employment which detail technical expertise gained through government employment in classified or sensitive programs.) Submit pre-publication requests to the supporting SSO for initial review and disposition. Additionally, the requirement for pre-publication review is part of an annual security education program. If the MAJCOM SSO has a question whether SCI material is included or not, the draft is forwarded, by secure means, to 25AF/SO for final review and disposition. 25AF/SO provides a classification decision, and returns the decision to the MAJCOM SSO within calendar 30 days. If the material is proposed for public release, formal Public Affairs approval is required IAW AFI 35-102, *Security and Policy Review Process*. The member initiates this process with the appropriate first-level Public Affairs office.

#### **4.6. Marking Classified Documents.**

4.6.1. All intelligence products, classified documents, and presentations (hard copy and electronic) is properly marked IAW Executive Order 13526, *Classified National Security Information*, ICD 710, *Classification and Control Markings System*, and as indicated in the *Intelligence Community Authorized Classification and Control Markings Register and Manual*. For additional information on marking requirements refer to the Security Markings Program (SMP) located on the ODNI Intelink resources page.

4.6.2. Derivative classifiers receive training reinforcing the importance of accountability and accuracy of their work at least once every two years. The MAJCOM SIO includes this requirement in the command's training for intelligence personnel. Derivative classifiers who do not receive training shall have their derivative classifier authority suspended until they receive training. To assist, CAPCO has an IC marking system web-based training (WBT) at <http://www.ncix.gov/training/wbt.php>. Go to Classification Management WBT.

4.6.3. Derivative classifiers performing derivative classification include an IC element POC and contact instructions at the end of all intelligence products to expedite decisions on information sharing.

**4.7. Classified Coversheets.** Coversheets prevent unauthorized viewing of classified documents and should be used whenever necessary.

4.7.1. Coversheets for all security classifications and SCI compartments may be downloaded from the DIA SCI JWICS webpage at <http://www.dia.ic.gov/homepage/security.html>.

4.7.2. To allow additional control markings/program identification, units may utilize locally reproduced/created classified coversheets provided they follow the format and color scheme of the DIA coversheets.

**4.8. DIA CAB.** DoDM 5105.21, V-1 requires organizations with a requirement for SCI intelligence to be listed in the DIA CAB. Each SSO with a CAB account validates their information contained in the CAB annually, and locally maintain documentation of that review.

## CHAPTER 5

### SECURITY INCIDENTS

**5.1. Overview.** This chapter covers the reporting procedures for SCI Security infractions, violations or inadvertent disclosures. **Note:** Security incidents involving NATO classified information is handled IAW AFI 31-406 **Chapter 8**. The POC for NATO related security incidents is SAF/AAZI.

5.1.1. Commanders, suspend access to SCI when information exists raising a serious question as to the individual's ability or intent to protect classified information, provided that the commander follows procedures in DoD 5200.2-R, paragraph C 8.1.3.

5.1.2. Commanders consult with your servicing legal office for advice on disciplinary issues for military member, labor law issues for civilian employees, and contract issues for contractors.

#### 5.2. Initial Reporting.

5.2.1. Persons who discover an SCI-related security incident will protect any SCI present and notify an SCI security official immediately (T-0).

5.2.1.1. SCI security officials report all SCI security incidents via secure means within 24 hours or the next duty day. The standard for reporting all security violations/infractions and ensuring correspondence by email or message to their servicing SSO, MAJCOM SSO, and AF CSA ([A2ZS.workflow@actnet.ic.gov](mailto:A2ZS.workflow@actnet.ic.gov)). The MAJCOM SSO will assign an incident number and forward the report to AF CSA via email (T-1). For security incidents occurring within the HQ MAJCOM SSO, the MAJCOM SSO reports the incident to the AF CSA who assigns an incident number. Refer to Figure 5.1, *Initial Report of Security Incidents*.

**Figure 5.1. Initial Report of Security Incidents.**

SAMPLE INITIAL REPORTING OF SECURITY INFRACTION/VIOLATION
(CLASSIFICATION depends on content)
FROM: Reporting SSO
TO: MAJCOM SSO SSO USAF//A2RS-CSA
SUBJ: Initial Notification of SCI Security Infraction/Violation and Request for Case Number
1. Unit name and geographical location of infraction/violation.
2. Date and time of infraction/violation.
3. Summary of infraction/violation and initial compromise determination if there is one suspected. Determination can be changed when final report is submitted.
4. Inquiry or investigative official appointed?
5. Point of contact, phone number and JWICS E-mail address.
<b>Note:</b> May be sent via message or JWICS E-mail.

5.2.1.2. For all security incidents determined to be a security violation; SSOs provide a preliminary assessment of the compromise determination in the initial report. Compromise determinations are:

5.2.1.2.1. Compromise Certain. SCI has irretrievably left SCI control channels; uncontrolled dissemination can be confirmed. Examples include a violation in which SCI appears in a newspaper or other public media, or SCI is known to have been seen by a foreign national or non-SCI accessed US citizen, who there is reason to believe shall not protect the information. When a SCI eligible non-indoctrinated person views SCI, the security violation shall not be considered a certain compromise if there is reason to believe the information shall be protected.

5.2.1.2.2. Compromise Probable. SCI has left SCI control channels; uncontrolled dissemination may reasonably be expected to occur, but a specific threat cannot be identified. For example, an SCI document found lying on a busy street would be a probable compromise because there is no way of knowing if anyone saw the document. Cases in which the investigator suspects SCI has been exposed to unauthorized personnel, but believe that further inquiry draws undue attention to the information, is also a probable compromise. An example of this situation is the discussion of SCI information in the presence of non-SCI-indoctrinated individuals. In this instance, the administration of inadvertent disclosure agreement would be appropriate. The transmission of SCI in an unclassified Record Message Traffic (RMT), on information technology (IT) systems or other electronic media devices given worldwide distribution could also fall into this category.

5.2.1.2.3. Compromise Possible. The possibility of uncontrolled dissemination of SCI cannot be ruled out, but with no specific indication to believe such dissemination takes place. A lost document containing SCI or SCI materials found in a non-secure location may represent a possible compromise. Transmission of SCI in a RMT message might also fall into this category if distribution was limited, if the message were classified either SECRET or CONFIDENTIAL, if SCI were placed on an internal, non-Internet connected IT system, or if the SCI is unlikely to be recognized.

5.2.1.2.4. Compromise Improbable. These are cases in which uncontrolled SCI dissemination is unlikely, but cannot be positively ruled out. This category includes exposure of SCI to unauthorized persons where an inadvertent disclosure agreement has been executed, or where the personnel exposed are SCI eligible, but not indoctrinated for the material. Compromise improbable also includes cases in which the investigator is satisfied that an unauthorized person is not aware of exposure or is unlikely to remember the SCI material; where SCI material is sent through the US Postal System but the material is double wrapped, the packaging shows no sign of tampering, and the material is delivered without undue delay. Another example is a case where it is improbable, but not certain, that the material ever left SCI control channels.

5.2.1.2.5. Compromise None. It is certain that SCI did not leave SCI control channels and was not exposed to unauthorized personnel. SCI found unsecured in a SCIF not authorized open storage may fall into this category. Compromise none also applies to individuals who have a valid TOP SECRET clearance, are indoctrinated for a category of SCI, and are inadvertently exposed to one or more SCI categories for which they are not indoctrinated.

5.2.1.3. AF CSA reports security violations and unauthorized disclosures determined to be compromises certain to DIA/SEC and SAF/AAZ respectively.

5.2.1.4. The SSOs will notify the appropriate Facility Security Officer and/or CSSO and the COR of any incident which involves a contractor/consultant (T-1).

5.2.1.5. Each MAJCOM will develop a unique numbering system identifying the command, calendar year and case number for example, ACC-SV-2013-001 (T-1).

5.2.1.6. Use the procedures in AFI 16-1404, to initiate/conduct preliminary inquiries/investigations. **Note:** For SCI incidents, the SIO, or designee, is the appointing official of the inquiry/investigating official and all reports are delivered to the SIO via the SSO.

5.2.1.7. SSOs will provide inquiry/investigation updates at least every 30 days to the MAJCOM SSO and AF CSA via email (T-1).

5.2.2. Reporting non-SCI incidents. Collateral intelligence information infraction/violations, occurring within the SCIF, is reported to the SSO. The MAJCOM SSO responds back to the notifying SSO assigning a case number to the security infraction/violation. Collateral violations that are determined not to contain intelligence data are turned over to the IP office.

**Figure 5.2. Assignment of Security Incident Number.**

<b>SAMPLE ASSIGNMENT OF SECURITY INCIDENT NUMBER</b>
(CLASSIFICATION DEPENDENT ON CONTENT)
FROM: MAJCOM SSO
TO: NOTIFYING SSO
SSO USAF//A2ZS-CSA//
SUBJ: Assignment of SCI Security Violation Case Number
REF: The Notification Message or JWICS E-mail
1. We have received and reviewed referenced initial security violation report. The following case number is assigned CASE NUMBER. The suspense for the final report is DATE. (30 days from the date of this msg. If all actions cannot be completed by the suspense date you must send a status report every 30 days until you forward the final report.
2. Upon completion of all actions, a final report will be completed.
3. Point of contact, phone number and JWICS E-mail address.
<b>Note:</b> May be message or JWICS Email.

### 5.3. Final Report.

5.3.1. The MAJCOM SSO adjudicates all security infraction/violations initiated within their command. The AF CSA adjudicates security infractions/violations that directly involve the MAJCOM SSO. The adjudication is based on the information in the final report. If the report contains insufficient, unintelligible, or conflicting information, the MAJCOM SSO or AF CSA requests additional/clarifying information from the submitting agency.

5.3.2. Following satisfactory adjudication of a case, the MAJCOM SSO will concur with or revise the incident compromise determination and close the case (T-1). The AF CSA reserves the right to make a final ruling on case closure and infraction/violation categorization or compromise determination.

5.3.3. SCI incidents cannot be closed by the local commander. All cases are to be reviewed and closed by the MAJCOM SSO and forwarded to the AF CSA for review.

**Figure 5.3. Final Security Incident Report.**

<b>SAMPLE FINAL REPORT OF SECURITY INFRACTION/VIOLATION</b>
(CLASSIFICATION DEPENDENT ON CONTENT)
FROM: REPORTING SSO
TO: MAJCOM SSO AF/A2ZS-CSA
SUBJ: Final Report for SCI Security Infraction/Violation <u>CASE NUMBER</u>
REF: ALL DOCUMENTATION REGARDING THIS CASE
1. Unit Name and Geographical Location of Infraction/Violation.
2. Date/Time of Infraction/Violation.
3. Personnel involved including, rank, name, SSAN, organization, clearance and compartments.
4. Summary of infraction/violation as documented in the inquiry official's report. Include investigator's official rank, name, organization, clearance and compartments.
5. Security infraction/violation characterized as actual or potential compromise.
6. Corrective action taken.
7. Name of each person found culpable in the infraction/violation, disciplinary action taken (if any), and were any SIFs created as a result of the infraction/violation.
8. SIO's name, rank, duty title, organization and if the SIO concurs.
9. Point of contact, phone number and JWICS E-mail.
<b>Note:</b> May be via message or JWICS E-mail.

## CHAPTER 6

### PHYSICAL SECURITY

**6.1. Overview.** This chapter covers the physical security and protection of facilities for storing, processing, and discussing SCI.

**6.2. Sensitive Compartmented Information Facilities (SCIFs).** Physical security standards for the construction and protection of SCIFs are prescribed in ICD 705 and associated Intelligence Community Standards (ICS), from here forward referred to as ICD 705. DoD SCIFs are established according to ICD 705 and this manual.

6.2.1. SCIFs are designated as a Restricted Area or Controlled Area according to AFI 31-101. The SSO/CSSO lists the SCIF within the post or installation directive which defines and designates all local controlled areas and post outside the SCIF the proper English and foreign (overseas areas only) language Restricted Area/Controlled Area signs as appropriate. If a SCIF is physically located within a restricted area, it does not need to be designated as a controlled area.

6.2.2. Restricted and Controlled Areas. SCIFs designated as USAF Protection Level (PL) 1, 2 or 3 resources are located in restricted areas and SCIFs designated as PL 4 are located in controlled areas. All SCIFs are protected and secured according to DoDM 5105.21, Volume 1-3 and AFI 31-101.

**6.3. Co-Utilization of SCIFs.** MAJCOM SSOs are the approving authorities for co-utilization of subordinate AF SCIFs. Use the format in DoDM 5105.21, Volume 2, to request SCIF co-utilization approval. Submit request through the local or supporting SSO to the MAJCOM SSO. Include the proposed Co-Utilization Agreement (CUA) with approval request. Request proposals and approval documentation will be maintained in the co-utilized SCIF for duration of the agreement (T-1).

**6.4. Special Access Programs (SAPs) Within DIA Accredited SCIFs.**

6.4.1. The approval authority for SAPs in SCIFs is the MAJCOM SIO. This authority cannot be delegated. AF CSA approves CUAs that occupy multiple AF SCIFs. MAJCOM SSO negotiate the CUA with their MAJCOM SAP security counterpart. AF CSA negotiates the CUA, as needed, with the appropriate service level SAP Controlling Office. Approvals for SAPs within AF SCIFs are secured before introduction of the SAP into the SCIF. AF CSA ensures the CUA includes language that allows the CUA to be amended by the local SSO and SAP security officer to local security conditions.

6.4.2. Use the format below to request approval for introduction of SAP material within an AF SCIF. Ensure subject and content of approval request is appropriately worded to specify it is a request for co-utilization of a SAP.

**Figure 6.1. SAP CUA Request.**

<b>SAMPLE SPECIAL ACCESS PROGRAM (SAP) CO-UTILIZATION AGREEMENT (CUA)</b>
CLASSIFICATION

FROM: (Unit desiring CUA and need for introducing SAP material into a SCIF)

TO: MAJCOM SSO  
AF/A2ZS-CSA

SUBJECT: Co-utilization Request

1. Identify the SCIF to be co-utilized (organization, room/building number, street address, city/state, zip code, SCIF ID number).
2. Identify the cognizant security authority.
3. Indicated the desired dates of co-utilization.
4. Indicate justification for introducing SAP material into the SCIF. If a defense contractor SCIF, indicate the contract number and CAGE Code as specified on the DD Form 254, and the expiration date.
5. Indicate all levels of SCI compartments required.
6. Indicated whether automated information system processing is required.
7. Indicate the number of personnel who occupy SCIF space.
8. Include a POC, office symbol and telephone number.

**Note 1.** MAJCOM SSO forwards co-utilization requests involving NSA, NRO, or CIA to DIA or NSA for approval (cc: AF CSA).

**Note 2.** Specific location of a SCIF associated with accreditation level is classified as a minimum at "CONFIDENTIAL."

**Note 3.** May be message or JWICS E-mail

## 6.5. SCIF Entry and Exit Inspections.

6.5.1. SCI security officials for AF SCIFs establish procedures for random inspections of hand-carried items entering or exiting SCIFs during operational hours. These procedures are to be part of the written Standard Operating Procedure (SOP) or Standard Practices and Procedures (SPP) for contractors. **Note:** SSOs/SSRs coordinate random inspection procedures with their local or MAJCOM legal office.

6.5.2. Outgoing Equipment Inspections. SSO/SSR/ISSO assigned to a SCIF physically inspect all outgoing equipment, furniture, and related items to prevent the unauthorized removal of classified information or accountable equipment. Inspections shall be performed by two persons and documented in writing (T-1). Retain documentation for one year after inspection.

**Figure 6.2. Furniture and Equipment Log.**

SAMPLE FORMAT FOR A FURNITURE AND EQUIPMENT INSPECTION LOG					
Date	Furniture or Equipment	Make & Model	Serial #	Inspector's Name	Inspector's Name

6.5.3. PED/Portable Computing Devices and Information System. The use of PEDs in a SCI environment presents a high degree of risk for the compromise of classified or sensitive information. IC Tech Spec, *Technical Specifications for Construction and Management of Sensitive Compartmented Facilities*, provides detailed instructions for the introduction/removal, approval requirements, handling, and connecting procedures for government owned PEDs, personally owned PEDs, contractor business owned PEDs, and all Information Systems.

6.5.3.1. DIA Memorandum, *Policy Clarification, Portable Electronic Devices, Introduction and Use of Personal Wearable Fitness Devices and Personal Headphones* and Code of Federal Regulations Title 47 Chapter I, 15.3, *Electronic Code of Federal Regulations, Section (3) (i) Definition for Class B device*, align the AF IC community with the rest IC on guidance related to the introduction and usage of personal wearable fitness devices (PWFDs) (i.e., FitBit© and other like commercially available devices), identified within the above references. MAJCOM SSOs will:

6.5.3.1.1. Develop command-level guidance using the below listed procedures for facilities under their cognizance before authorizing PWFDs into SCI facilities (T-1). Command level guidance is provided to the AF CSA for review and approval before implementation.

6.5.3.1.2. Develop and implement PED guidance for facilities within their MAJCOM that are tailored to their specific organization and mission (T-1).

6.5.3.1.3. Review and approve planned acquisitions of government-issued PEDs as part of the component's Supply Chain Risk Management program (T-1).

6.5.3.1.4. In coordination with ACC/A2S, approve requests for authorization to connect government-issued PEDs to a system (T-1). These authorizations are kept to the minimum required to accomplish the organization's mission.

6.5.3.1.5. Develop and provide initial and annual Cybersecurity Awareness training for personnel to address current PED vulnerabilities and threats (T-1).

6.5.3.2. MAJCOM SSOs are the sole approval authority for introduction of prohibited items identified in ICD 705. MAJCOM SSOs may delegate this authority at their discretion. The MAJCOM SSO will:

6.5.3.2.1. Coordinate any waiver that impacts physical or TEMPEST accreditation with DIA/SEC for approval and a courtesy copy is sent to AF CSA (T-1).

6.5.3.2.2. Ensure waivers involving Information Systems are reviewed by the MAJCOM Command Information Systems Officer (CISO) and sent to ACC/A2XI for approval (T-1). Waivers are valid for up to one year.

6.5.3.2.3. Ensure the facility security officials are familiar with applicable guidance on prohibited electronic equipment (T-1). Prohibited items found within these facilities are confiscated for a review by AFOSI. SIO is notified when prohibited items are required because of mission, medical, or occasion use. The following items are prohibited within facilities.

**Figure 6.3. Prohibited Electronic Equipment.**

<b>Prohibited Electronic Equipment</b>
Non-government photographic (to include camera telephones), video, and audio recording equipment
Non-government computers and associated media
Non-government two-way radios, cell phones, pagers with transmit capability
Non-government diagnostic equipment
Non-government weapons
Hazardous materials (e.g. acids, caustic materials, gasoline, etc.)
Illegal contraband

6.5.3.3. The Commander or Senior Civilian responsible for the facility will:

6.5.3.3.1. Authorize government-issued PEDs to be used in facilities when it is in support of a mission (T-1).

6.5.3.3.2. Authorize contractor-supplied PEDs to be used in facilities when it is in support of AF contracts, in coordination with the Contracting Officers Representative (COR) (T-1). Refer to Figure 6.4. *Facility Authorization Letter*.

6.5.3.3.3. Direct security investigations in response to known or suspected violations (T-0).

6.5.3.3.4. Confiscate any PEDs (government-issued, contractor-supplied or personally owned) which are unauthorized or used in a manner inconsistent with this guidance (T-0).

6.5.3.3.5. Consult the supporting AFOSI in response to known or suspected violations of this guidance (T-1).

6.5.3.3.6. Establish secure PED storage areas for visitors and commuters (T-0). Security Officers affix a sign in a prominent place containing the following: “By bringing a Portable Electronic Device (PED) into this facility, the User agrees that the US Government, or its representative, may seize the PED for physical and forensic examination at the government's discretion. Use of this locker constitutes consent to examination, inspection, and search of its contents by authorized security or other personnel in the conduct of their duties. Claims for loss for damage to personal items stored in this locker should be filed through applicable Service claims authorities.”

6.5.3.3.7. Ensure all government-owned PEDs are affixed with a tamper seal (T-0).

6.5.3.4. Information Systems Security Officer will:

6.5.3.4.1. Ensure the execution of Cybersecurity policies for applications, information technology (IT) resources, and networks (T-1).

6.5.3.4.2. Approve the insertion or connection of any PEDs to IT resources only after approval by the SIO and other authorizing officials (T-1).

6.5.3.4.3. Monitor systems for rogue and unauthorized devices accessing networks (for example, Host-Based Security Systems) and report PED use and violations within the facility to the local SSO or Special Security Representative (SSR) (T-1).

6.5.3.4.4. Coordinate on requests authorizing the hand-carrying of government-issued and contractor-supplied PEDs into and out of facilities (T-1).

6.5.3.4.5. Provide Information Systems technical guidance for the use and security of authorized PEDs (T-1).

6.5.3.5. Security Officials (SSO, CSSO, SSR and CSSR) will:

6.5.3.5.1. Develop standard operating procedures (SOP) within the Facilities SOP for the introduction and use of PEDs (T-0).

6.5.3.5.2. Monitor, track, and authorize the entry and removal of government-issued and contractor-supplied PEDs (T-0).

6.5.3.5.3. Authorize the entry and removal of personally-owned PEDs, IAW Figure 6.4, *Facility Authorization Letter*, by SCI-cleared civilian, military, contractor and visitors (T-0).

6.5.3.5.4. Maintain accurate records on government-owned and contractor-supplied PEDs authorized within the facilities (T-0). Records include the PED manufacturer, model number, serial number, contract number, and expiration date as applicable. Records for government-issued PEDs are maintained for the life of the device. Records for contractor-supplied PEDs are maintained until the contract expires or the contractor is no longer assigned on the contract.

6.5.3.5.5. Conduct random inspections to identify violations (T-0).

6.5.3.5.6. Report violations of this guidance to the Site Information System Security Manager (ISSM) and SIO (T-0).

6.5.3.5.7. Collaborate with Technical Security Counter-Measures (TSCM) personnel to perform electronic monitoring to determine if unauthorized PEDs are being used (T-1).

6.5.3.5.8. Ensure all authorized PEDs are affixed with the manufacturer's tamper seal and/or an AF-approved tamper seal prior to employment within the SCIF (T-0).

6.5.3.6. Contracting officer's representative (COR) will:

6.5.3.6.1. Validate contractor-supplied PEDs serve a justified mission requirement in support of AF contracts, and ensure devices and usage are documented within the Statement of Work (SOW), Statement of Objectives and annotated, in the Department

of Defense Form 254, *Department of Defense Contract Security Classification Specification* (T-0).

6.5.3.6.2. Validate requirement for issuance of a property pass to affiliates carrying contractor-supplied PEDs in and out of facilities in support of an AF contract (T-0).

6.5.3.6.3. Ensure authorized contractor-supplied PEDs are affixed with a tamper seal (T-0).

6.5.3.7. Civilian, military, contractor, and visitors:

6.5.3.7.1. Be approved by the facility SSO prior to being introduced into facilities (T-0). The signed user agreement with SSO approval is kept with the PED (T-0).

6.5.3.7.2. PEDs that are authorized are allowed to be used within a facility IAW this guidance and local policies, in areas identified by the SSO as unclassified or common areas. Examples may include lobbies outside facilities turnstiles, cafeterias, fitness centers, and patios. PEDs in common areas do not require SSO approval and may be taken in and out of the areas as needed (T-0).

6.5.3.7.3. Not connect PEDs to telecommunications networks, IT resources, telephone, or Ethernet without prior written authorization from the Site ISSM (T-0).

6.5.3.7.4. PEDs that are not authorized (for example, those PEDs with audio, video, photographic, or wireless capability) are turned off and stored outside the facilities, in a vehicle, or a storage locker before the employee enters facility (T-0).

6.5.3.7.5. Not use recording capabilities of personally-owned PEDs within any facility unless approved IAW with this guidance (T-0).

6.5.3.7.6. Civilian, military employees and visitors may request to use personally owned cameras (excluding telephones with camera capabilities, as cellular telephones are prohibited) or PEDs with an embedded photography or video capability for special events, such as ceremonies. These requests go through the event coordinator, who forwards a consolidated request to the SSO. The SSO provide the approval letter to the access control point of their facility with copies provided to the requestors. Approved devices may be carried through general common areas to reach a specified approved use area provided the photography or video capability is turned off or not used.

6.5.3.7.7. Obtain documentation for hand carrying government-issued and contractor-supplied PEDs in and out of the facilities. The documentation includes the make, model, and serial number, of the PED (T-0).

6.5.3.7.8. Maintain property documentation with authorized government-issued and contractor-supplied PEDs at all times (T-0).

6.5.3.7.9. Maintain a copy of the Facility Authorization Letter, signed by the SSO and Site ISSM, for the specified contractor-supplied PED at all times (T-0).

**Figure 6.4. Facility Authorization Letter.**

<b>Facility Authorization Letter Example</b>	
TO:	
FROM: [Name of contractor requesting to introduce Contractor-supplied PED(s)]	
SUBJECT: Authorization to bring Contractor-supplied Portable Electronic Devices in and out of AF SCIF XX-XX-XXX	
<p>1. IAW the above Reference, contractor-supplied portable electronic devices (PEDs) which have a capability to perform any of the following: store, record, or transmit (radio frequency or infrared) data, digital images, video, or audio are prohibited in any government issued or leased SCIFs unless authorized IAW the reference. Examples of these devices include, but are not limited to, amplitude modulation (AM), frequency modulation (FM), satellite radios, two-way pagers, laptop computers, mobile telephones, personal digital assistants (such as palm tops, Blackberry, iPhone, Android, iPAQ, iPad), digital audio devices (such as MP3 players, iPods), digital or film cameras, digital or tape camcorders, electronic book readers (such as Kindles, Nooks, Neo's), digital picture frames, electronic watches with input or recording capability, and voice recording devices.</p> <p>2. Contractor-supplied PEDs are authorized within (facility ID #) provided the PED serve a justified mission requirement, and:</p> <p>a. Justification and usage is documented in the Statement of Work/Statement of Objectives (SOW/SOO),</p> <p>b. Are listed on the DD Form 254, <i>Department of Defense Contract Security Classification Specification</i>, and</p> <p>c. Will never be connected to classified telecommunications networks, information systems, telephony, or Ethernet, to include charging the device via universal serial bus ports.</p> <p>3. You are hereby authorized to bring the following PED(s) into and out of facilities in order to perform a justified mission requirement in support of contract (number), period of performance (from date -to date):</p>	
Item/Type Make/Model Serial Number	
SSO/CSSO Name	CISO/ISSM
Division/Organization	Division/Organization
Contact phone number	Contact phone number
SSO/CSSO Signature	CISO/ISSM Signature

6.5.3.7.10. Maintain a copy of the User Agreement for Personal Portable Electronic Devices, signed by the SSO for the specified personal PED that is authorized for introduction into a facility (T-0).

**Figure 6.5. User Agreement for Personal Portable Electronic Devices (PED).**

<b>USER AGREEMENT FOR PERSONALLY OWNED PORTABLE ELECTRONIC DEVICES</b>		
LAST NAME _____ FIRST NAME _____ INITIAL _____ RANK/GRADE _____ POSITION _____ UNIT _____ DUTY PHONE _____		
<p>I. (U) By my signature below, I acknowledge that;</p> <p style="margin-left: 40px;">a. I understand my responsibilities and will comply with procedures set forth in the Portable Electronic Devices policy.</p> <p style="margin-left: 40px;">b. I understand that the U.S. Government (USG) through a designated representative of the Department of Defense (DoD) may seize my personal portable electronic device (PED) for security purposes and that the USG or its designee may conduct a physical and forensic examination of the PED. I understand that PEDs seized as evidence of a crime or security violation will be handled under DoD Investigative Policies. In some cases, PEDs may be permanently retained, destroyed, or have their data and operating systems wiped resulting in loss of information.</p> <p style="margin-left: 40px;">c. I understand that if I have a legitimate claim for loss or damage to a personal PED, not lost or damaged through my own negligence or violation of security procedures that may file a claim in accordance with claims procedures administered by the Air Force.</p> <p style="margin-left: 40px;">d. I am fully aware that it remains my inherent responsibility as an AF Employee, or member of the armed forces assigned to AF, to fully protect all Sensitive material in my custody, ensuring against loss or compromise. Nothing in the foregoing shall be construed to excuse my use of good judgment and common sense to provide maximum security protection of the information entrusted to my possession.</p> <p style="margin-left: 40px;">e. I understand that I am only allowed to bring in those devices approved by my Special Security Officer/Contractor Special Security Officer and annotated on this form.</p>		
_____ (Signature)	_____ (Date)	
<b>DEVICE</b>	<b>MODEL</b>	<b>SN</b>

<b>Special Security Officer/Contractor Special Security Office Acknowledgement/Approval</b>	
_____ (Printed Name)	_____ (Unit)
_____ (Signature)	_____ (Date)
<p><b>PRIVACY ACT STATEMENT</b>                  Authority: The National Security Act of 1947, as amended and DIA Instruction 8460.002 authorize collection of this information.</p> <p>Principal Purpose: The information is collected to provide Special Security Officers and Contractor Special Security Officers ability to manage employee use of PEDs.</p> <p>Routine Uses: The information is collected to provide Special Security Officers and Contractor Special Security Officers ability to manage employee use of PEDs.</p> <p>In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the Department of Defense as a routine use pursuant to 5 U.S.C.552a(b)(3) as follows:</p> <p>The DoD 'Blanket Routine Uses' set forth at the beginning of the Defense Intelligence Agency's compilation of systems of records notices apply to this system.</p> <p>Disclosure: This information is requested on a voluntary basis. However, not providing the information could have an impact on determining PED use eligibility.</p>	

- 6.5.3.7.11. Not tamper with or alter any affixed tamper seal applied to an authorized PED (T-0).
- 6.5.3.7.12. Protect PEDs from unauthorized access and theft (T-0).
- 6.5.3.7.13. Transport (hand carry) and use only authorized government-issued and contractor-supplied PEDs in the facility for authorized purpose(s) IAW this guidance (T-0).
- 6.5.3.7.14. Successfully complete initial and annual Cyber security Awareness training (T-0).
- 6.5.3.7.15. Report violations or suspected violations of this guidance to their organization's security officer or SSO (T-0).

6.5.3.7.16. Exercise prudent measures whenever using, transporting, or storing PEDs to reduce operational security indicators that may divulge AF activities or facilities (T-0).

6.5.3.8. Introduction and Usage of Personal Wearable Fitness Devices (PWFDs). DIA as the accrediting authority for AF SCIFs has determined that PWFDs are not authorized for facilities located outside the continental US (Hawaii and Alaska are considered continental US) (T-0).

6.5.3.8.1. PWFDs that are authorized for introduction and use within AF SCIFs and facilities located in the continental US (Hawaii and Alaska are considered continental US) operating with a co-use agreement under the following circumstances:

6.5.3.8.1.1. Commercially available in the US or through the US military exchanges (T-0).

6.5.3.8.1.2. Marketed primarily as a fitness device (T-0).

6.5.3.8.1.3. Designated as a Federal Communication Commission (FCC)-Class B digital device. Note: FCC-Class B designations can be obtained in two ways and perhaps advertised in either manner by manufacturers: FCC-Class B "certified," or FCC-Class B "exempt."

6.5.3.8.2. Facilities creating co-use agreements between agencies will address the introduction of PEDs within the agreement (T-1). Facilities where co-use agreements already exist use the most stringent PEDs guidance codified within each agency. The device can not contain the capabilities or characteristics IAW Figure 6.6, *Device Prohibited Capabilities or Characteristics*.

**Figure 6.6. Device Prohibited Capabilities or Characteristics.**

<b>Prohibited Capabilities or Characteristics</b>
Cellular connectivity
Wi-Fi capabilities
Photographic or video capture/recording capabilities
Microphone or audio recording capabilities
<b>Note:</b> Bluetooth© is a wireless capability but is not the same as Wi-Fi. Bluetooth capability is considered low risk. PWFDs with Bluetooth© are allowed.

6.5.3.8.3. Personally owned PEDs without audio or video recording, photographic capabilities, or wireless transmitting capabilities are authorized in facilities IAW the paragraphs below. These devices include: MP3 players, calculators, vehicle keys, RF remote openers that are push to operate, clocks, AM/FM radios, cassette and compact disk players, spell checkers, language translators, receive only pagers, health monitors, and headphones (without embedded microphone and noise canceling technology). Only fitness devices with Bluetooth technology are allowed providing they do not have an audio, video, photographic or other wireless capability (i.e. Wi-Fi). The devices listed above are considered low risk because they do not possess restricted or prohibited functionalities. **Note:** Fitness devices cannot be within the proximity of the Bluetooth connection when inside a SCIF.

6.5.3.8.3.1. Government-issued and contractor-supplied PEDs are allowed within facilities IAW this guidance, the Facility SOP, and when specific written approval from the Commander or the Senior Civilian Official has been given for each item (T-0).

6.5.3.8.3.2. Request for authorization to connect government-issued and contractor-supplied PEDs to a system is approved by the Commander or the Senior Civilian Official, then the SIO, with the final approval from the IT Networks Accrediting Authority (T-0).

6.5.3.8.3.3. Government-issued and contractor-supplied PEDs is clearly marked and inventoried when authorized for use in facilities (T-0). While in the facilities and not in use, the government-issued and contractor-supplied PED is stored in a secure location (such as in a cabinet or locker, or secured by cable) (T-0).

6.5.3.8.3.4. Government-issued PEDs, which contain Privacy Act, classified, or controlled unclassified information, encrypted with a National Security Agency or Department of Defense-approved encryption standard to the level of supported classification (T-0).

6.5.3.8.3.5. Contractor-supplied PEDs used in support of AF contracts are subject to the same restrictions as government-issued PEDs. Contractor-supplied PEDs and their intended usage is included in the SOW and documented in a DD Form 254 or else it is treated as personally owned (T-0).

6.5.3.8.3.6. Purchases of government-issued PEDs are coordinated jointly with the organization's Cybersecurity Office, SSO, SIO, and Equipment Custodian Officer (ECO) to ensure potential vulnerabilities and mitigation strategies are addressed prior to the expenditure of funds (T-0).

#### 6.5.3.8.4. Foreign owned PEDs:

6.5.3.8.4.1. Foreign national personnel assigned to AF organizations under formal government-to-government agreements are considered to be AF affiliates and follow the requirements listed for civilian and military employees (T-0). Their PEDs are limited to those areas in which they have unescorted access (T-0).

6.5.3.8.4.2. PEDs in the possession of foreign visitors are not allowed into any AF facility. This includes any foreign national affiliates and contractor-supplied devices (T-0). Foreign visitors requiring the use of a PED such as an electronic translator use a US Government-provided device and the device remains in the custody of the US Government (T-0).

6.5.3.8.4.3. Foreign visitors found with a PED in their possession beyond the facilities entrance are escorted back to the entrance of the facility and instructed to secure the PED or they are not allowed into the facility (T-0). The incident is reported as a security incident (T-0).

#### 6.5.3.8.5. Personally owned PEDs.

6.5.3.8.5.1. Are never connected to information system resource to include re-charging (T-0).

6.5.3.8.5.2. Are not allowed in DoD SCIFs located overseas on or off a military installation or compound.

6.5.3.8.5.3. Never allowed in DoD SCIFs to include a US military installation or compound if Wi-Fi technology is a part of the device, regardless whether or not the function can be manually turned off (T-0).

6.5.3.8.5.4. That are taken overseas on TDY/Deployment/Personal travel are not allowed into DoD SCIFs upon return to the US if positive control was not maintained (of the PED) at all times. PEDs taken overseas are not reintroduced into facilities upon return to the US unless it undergoes a physical/forensic examination. It is incumbent on the user/owner of the PED to understand this requirement prior to introduction into a facility. If possible, this should also be conducted prior to being taken overseas to establish a baseline. If the PED is brought into the facility prior to examination a security incident is initiated (T-0).

6.5.3.8.6. Accountability of Government-Issued and Contractor-Supplied PEDs. PEDs are subject to the capability restrictions described in Figure 6.7, *Portable Electronic Device Prohibited Capabilities Matrix* and require the appropriate documentation for entry into and removal from facilities.

**Figure 6.7. PED Prohibited Capabilities Matrix.**

<b>PORTABLE ELECTRONIC DEVICE PROHIBITED CAPABILITIES MATRIX</b>		
<b>CAPABILITY</b>	<b>EXAMPLES</b>	<b>NOTES</b>
Photographic	Cameras, cellular telephones/Smartphones with built in camera, iPods/iPads/tablets with built in camera, etcetera	Government only devices are allowed but cannot be used in AF restricted or SCIF areas without approval. Must be turned off and placed in an RF bag. Exceptions may be granted IAW this issuance.
Video Recording	Video cameras, cellular telephone/Smartphones with built in camera, iPods/iPads/tablets with built in camera, webcams, etcetera	Government only devices are allowed but cannot be used in a restricted or SCIF areas without approval. Must be turned off and placed in an RF bag. Exceptions may be granted IAW this issuance.
Audio Recording	Cellular telephones/Smartphones, laptops, cassette recorders, iPods/iPads/tablets with the ability to record external audio, etcetera	Government only devices are allowed but cannot be used in a restricted or SCIF areas. Must be turned off and placed in an RF bag.

Radio Frequency (RF) Wireless transmit capability	All cellular telephones and Smartphones, sports watches with wireless capability, iPods/iPads/tablets with wireless capability, any device with Bluetooth or other 802.11 and 802.15 capabilities.	Government only devices are allowed in but cannot be used in AF restricted or SCIF areas and must be turned off and placed in an RF bag. Must be controlled by the Information Systems Manager and/or SSO. Removable wireless access cards contained within government-issued or contractor-supplied laptop computers must be removed prior to introduction into restricted of SCIF spaces. Car key fobs are excluded from this restriction.
Infrared (IR) Wireless transmit capability	IR remote controls	Government only devices are allowed in but cannot be used in restricted or SCIF areas, copper tape must be applied over IR ports. Infrared presenter devices which can convey no intelligence information are excluded from this restriction.
<p><b>Note:</b> The capabilities annotated in the matrix above are prohibited within all DIA accredited SCIF areas, unless explicitly approved IAW this guidance.</p> <p><b>Note:</b> Personally owned PEDs with these capabilities are prohibited. Government-issued and contractor-supplied PEDs may be allowed IAW this guidance and with written authorization from the AF Component SIO and, as required, ISSM. All devices are subject to inspection.</p> <p><b>Note:</b> If you are unsure if your device has a restricted capability, contact your organizations Security Official for questions regarding personally owned PEDs</p>		

6.5.3.8.7. PEDs are refreshed to a default factory setting to eliminate foreign intelligence entities targeting and potential malware on the anniversary of the user agreement (T-1).

6.5.3.8.8. Appropriate documentation is issued for government-issued or contractor-supplied PEDs. Tamper seals should be placed on each device prior to issue and contain some type of inventory device (T-0).

6.5.3.8.9. PEDs transported or used outside of the US, its territories, or possessions:

6.5.3.8.9.1. Be protected at all times. Users have positive physical control (that is, within eyesight) of government-issued and contractor-supplied PEDs. Failure to ensure control results in the device being restricted from facilities (T-1).

6.5.3.8.9.2. Undergo a physical/forensic examination prior to reintroduction into the facility. If possible, this should also be conducted prior to being taken overseas to establish a baseline (T-0).

6.5.3.8.10. PEDs introduced into facilities for Medical use, Emergency response or TEMPEST requirements:

6.5.3.8.10.1. Items needed by the disabled for medical or health reasons, such as motorized wheelchairs, hearing aids, heart monitors, pacemakers, and insulin pumps. Initial requests are sent to the organization's EEO office, which validate the request as an authorized reasonable accommodation. Approved requests are

sent to SSO to review the technical capabilities of the device to determine threats and mitigations. The SSO's recommendation is then sent to the requestor. Health or medical equipment, which requires connection to an IT resource, first is approved by the Network Designated Approval Accrediting Authority prior to their introduction into any facility. Personnel having questions regarding what type of medical equipment can be introduced into facilities without advanced approval should seek guidance from their element SSO or SSR.

6.5.3.8.10.2. Emergency and police personnel and their equipment, including devices carried by emergency medical personnel, responding to a medical crisis within a facility. Emergency personnel are admitted without regard to their security clearance status but are escorted to the degree practical (T-0). Emergency personnel are debriefed as soon as possible if there are any indications these individuals have been exposed to classified information or information systems (T-0).

6.5.3.8.10.3. Compromising emanations (TEMPEST) testing equipment or TSCM testing equipment, as long as the equipment is operated by authorized technical surveillance countermeasures or TEMPEST practitioners or technicians, and such practitioners or technicians possess the appropriate security clearances and indoctrinations.

#### **6.5.4. Misuse of PEDs or violation of the PED guidance.**

6.5.4.1. Unauthorized use of PEDs jeopardizes AF mission, IT resources, and information security. Violations of this guidance will be aggressively pursued (T-0). Unauthorized possession or use of any PED could result in its confiscation by officials for the purpose of conducting a forensic/physical examination (T-0).

6.5.4.1.1. Examination may result in exposure of all content and metadata residing on the PED. There is no reasonable expectation of privacy or confidentiality in the content and metadata resident on any and all PEDs brought into AF-controlled facilities.

6.5.4.1.2. Authorized examination of PEDs may result in data loss, compromise of functions, damage, or destruction of the PED. In some cases, PEDs may be permanently retained, destroyed, or have their data and operating systems sanitized.

6.5.4.1.3. In some cases, the PED may not be returned to the user.

6.5.4.2. Unauthorized use of any PEDs may result in administrative, investigative, disciplinary, or prosecutorial action. This may include, but is not limited to:

6.5.4.2.1. Suspension of access to information systems (Non-Secure Internet Protocol Router Network, Secure Internet Protocol Router Network, Joint Worldwide Information Communications System, or other DoD-affiliated systems, such as contractor systems operated by DoD).

6.5.4.2.2. Personnel being placed on administrative leave pending investigation of the security violation.

6.5.4.2.3. A permanent entry placed in the person's personnel security file.

6.5.4.2.4. Termination of duty, disciplinary action under the Uniform Code of Military Justice, criminal prosecution, or other administrative or appropriate disciplinary proceedings for military, civilian, or contractor employees.

## 6.6. SCIF Accreditations and Inspections.

6.6.1. MAJCOM SSOs will communicate directly with DIA/SEC and courtesy copy the AF CSA on all matters concerning accreditations, inspections, and administrative issues pertaining to SCIFs under their purview (T-1). **Note:** This also applies to contractor-operated SCIFs.

6.6.2. DIA/SEC is the sole authority for accrediting DoD permanent SCIFs, excluding those under NSA, National Geospatial-Intelligence Agency (NGA) or National Reconnaissance Office (NRO) cognizance.

6.6.3. Below the MAJCOM level, the accreditation request is forwarded to the MAJCOM SSO for review, corrections and concurrence. Once approved, the MAJCOM SSO forwards the request to DIA/SEC. DIA grants interim accreditation pending a favorable physical and technical inspection by DIA or a DIA certified SCIF inspector assigned to the requesting MAJCOM.

6.6.4. Concept approval is required for all new SCIFs and signed by the MAJCOM SIO and then forward to DIA/SEC. Concept approvals clearly state the operational need for the new SCIF, estimated cost of construction, and include a declaration that the sponsoring organization has or intends to acquire the resources (e.g., personnel, funding) necessary to provide management and oversight for the new SCIF during its lifetime. The intent is to give leaders at MAJCOMs greater visibility on SCIF issues under their purview in order to better manage resources.

### Figure 6.8. Concept Approval.

<b>CONCEPT APPROVAL REQUEST SAMPLE</b>
<p>MEMORANDUM FOR: MAJCOM SSO AF/A2ZS-CSA</p> <p>FROM: Organization Requesting SCIF</p> <p>SUBJECT: (*) Request for Concept Approval</p> <ol style="list-style-type: none"> <li>1. (*) Identified the organization seeking accreditation and location of the proposed SCIF. Include the room number, street address, and address where classified mail is received.</li> <li>2. (*) Provide justification for establishment of SCIF. Identify the program/contract requiring the SCIF, what mission or operation is being supported, the required SCI compartments, and the type of storage required.</li> <li>3. (*) Advise when construction or modification of existing space is proposed. Explain why existing SCIF (in the general area) cannot be used.</li> <li>4. (*) Specify Information System/communications and SCI circuit requirements.</li> <li>5. (*) Provide the date the proposed SCIF is desired to be operational.</li> <li>6. (*) Provide the office symbol and telephone number of the POC.</li> <li>7. (*) For Federally funded Research Development Centers (FFRDCs) and Cooperative Research and Development Agreement (CDRAs), include a copy of the correspondence authorizing establishment of a SCIF.</li> </ol>

**SSO/CSSO/SSR SIGNATURE BLOCK****1 Attachment**

Attach a copy of the DD Form 254 for DoD contractor requests. Enter the contract expiration date in block 2a of the DD Form 254.

**Note 1.** Unit requesting establishment of a SCIF use this format. The request are classified at least "CONFIDENTIAL", derived from: SCI SCIF Accreditation Security Classification Guide, V1.0, 1 Oct 2012, Paragraph 11, Item 1.0, Declassify Upon Withdrawal of SCIF Accreditation.)

**Note 2.** Units submit requests to their supporting SSO to MAJCOM SSO for review and approval, with a copy to their supporting SSO for review/filing.

**Note 3.** If the unit is a DoD contractor, include a copy of the DD Form 254 with the Concept Approval request.

**Note 4.** The request is classified at least "CONFIDENTIAL," Derived From: SCI SCIF Accreditation Security Classification Guide, Version 1.0, 1 Oct 12, Paragraph 11, Item 1.0, Declassify Upon Withdrawal of SCIF Accreditation.

**Note:** In the following format sample “(\*) is the prompt to add the appropriate classification within the text of the document.

#### 6.6.5. SCIF Inspections.

6.6.5.1. MAJCOM SSOs nominate to AF CSA at least two MAJCOM personnel for certification as SCIF inspectors. Nominees possess the requisite knowledge to carry out SCIF inspections, gained through on-the-job experience and formal training (i.e. DIA’s SCI Security Official’s Course, or equivalent, and Director of National Intelligence [DNI] ICD 705 course, or equivalent). In instances where an otherwise-qualified person has not attended one of the formal courses, MAJCOM SSOs may coordinate a solution with AF CSA to obtain training and enable certification. DIA/SEC issue individual certificates of completion and DIA/SEC and AF CSA maintains a master list of certified SCIF inspectors.

6.6.5.2. When an inspection result in recommendations that require alteration of the physical or technical configuration of the SCIF, then prior to implementation, such recommendations are up-channeled and approved through the MAJCOM SSO, AF CSA, and DIA/SEC (T-0).

6.6.5.3. SCI Security Management and Self- Inspections. Each respective security official will submit copies of their annual self- inspections to their MAJCOM SSO, consolidate the results and forward a summary to the AF CSA (T-1). The intent is to reduce redundancy, and in turn increase overall responsiveness, by using already required self- inspections as certifications.

6.6.5.4. A SCIF must receive a favorable physical and TEMPEST accreditation inspection by DIA/SEC or a DIA/SEC certified SCIF inspector assigned to the respective MAJCOM prior to accreditation (T-0).

6.6.5.5. Unannounced after duty-hour security inspections are to be conducted IAW DoDM 5105.21-V2 at least annually on all MAJCOM SCIFs.

#### **6.7. Temporary Secure Working Areas (TSWA) and Temporary SCIFs (T-SCIF).**

6.7.1. DIA/SEC has delegated to the AF/A2 or designees the authority to accredit TSWAs and T-SCIFs. AF/A2 has designated MAJCOM SSOs as the accrediting authority for T-SCIFs and TSWAs in their areas of responsibility. MAJCOM SSO personnel are granted this authority in writing by the MAJCOM SIO. Additionally, those personnel appointed with this authority need to have a working knowledge of ICD 705 and the policies contained in DoDM 5105.21 and this manual.

6.7.2. A TSWA is a facility, room, or area used on a temporary or intermittent basis for handling, discussing, or processing SCI, but where SCI is not stored. The owning MAJCOM SSO is the TSWA approval authority (T-1). The AF SCI Authorizing Official and/or cognizant Delegated Authorizing Official is the approval authority for electronic processing of SCI within an approved TSWA.

6.7.2.1. When required all MAJCOM SSOs with TSWA designation authority will request a waiver of the 12 month restriction through DIA for designated Senior Leader offices. The waiver if granted is immediately terminated if the room no longer requires TSWA designation. TSWAs with waivers will be provided to the AF CSA within 30 days of approval, a complete list will be provided on a yearly basis thereafter when requested by the AF CSA (T-1).

**Figure 6.9. Temporary Secure Working Area (TSWA) Request.**

<b>TEMPORARY SECURE WORKING AREA (TSWA) REQUEST SAMPLE</b>
<p>MEMORANDUM FOR: MAJCOM SSO AF/A2RS-CSA</p> <p>FROM: Organization Requesting SCIF</p> <p>SUBJECT: (*) Request for Concept Approval</p> <ol style="list-style-type: none"> <li>1. (*) Identified the organization seeking accreditation and location of the TSWA. Include the room number, street address, and address where classified mail is received.</li> <li>2. (*) Identify a responsible security official and alternate. Provide their telephone and facsimile telephone numbers (both secure and non-secure).</li> <li>3. (*) Provide justification for establishment of TSWA. Identify the program/contract requiring the SCIF, what mission or operation is being supported, the required SCI compartments, and the type of storage required.</li> <li>4. (*) Provide the duration of accreditation (either date to date or annual).</li> <li>5. (*) Identify facility hours of operation.</li> <li>6. (*) Will SCI storage be required? If yes, submit justification. Describe how SCI material is stored. (Open store of SCI material in a TSWA is prohibited). Specify amount, location, and identification number of nearest SCIFs, and why SCI material cannot be stored inside the SCIFs.</li> <li>7. (*) Is the TSWA alarmed? If so describe the alarm system used.</li> <li>8. (*) Are sound attenuation requirements met? Provide sound transmission class (STC) rating. Include information of doors, vents, sound baffles, and air handling system as necessary.</li> <li>9. (*) Types of locks on doors.</li> </ol>

10. (\*) When not in use at the SCI level, is access to the TSWA limited to personnel possessing at least a U.S. SECRET clearance? The TSWA must be controlled at the U.S. SECRET level when not in use as a TSWA.
11. (\*) Is there any electronic processing of SCI within the TSWA? If yes, provide a list of the equipment used showing manufacturer, model number, and processing level.
12. (\*) Will SCI presentations via standalone SCI computers be required? If yes, submit TSWA computer SOP.
13. (\*) Telephones installed within the TSWA should meet the requirements outlined in ICD 705.
14. (\*) Organizational POC and phone telephone number.
15. (\*) Servicing SSO POC and telephone number.

#### REQUESTOR SIGNATURE BLOCK

##### 1 Attachment

Attach a copy of the DD Form 254, DoD Contract Security Classification Specification, for DoD contractor requests. Enter the contract expiration date in block 2a of the DD Form 254.

**Note 1.** Unit requesting establishment of a TSWA must use this format. Once completed, the document becomes at a minimum, “CONFIDENTIAL.”

**Note 2.** Units should submit this request to their MAJCOM for review and approval, with a copy to their supporting SSO for review/filing.

**Note 3.** If the unit is a DoD contractor, include a copy of the DD Form 254 with the Concept Approval request.

**Note 4.** The request must be classified at least “Confidential” and Derived From: DoDM 5105.21, Declassify Upon Withdrawal of SCIF Accreditation.

**Note 5.** Paragraph 3 of the memorandum is classified as a minimum at “CONFIDENTIAL”.

**Note 6:** (\*) is the prompt to add the appropriate classification within the text of the document.

6.7.2.2. During contingencies, if immediate JWICS capability is warranted to accomplish the war-time missions, the AF SCI Authorizing Official and/or cognizant Delegated Authorizing Official is the approval authority for a JWICS signal line to run from an accredited SCIF to the TSWA via a protected distribution system (PDS). The JWICS signal line and circuit is removed immediately after completion of the mission. Request for approval will be staffed through ACC/A2XI (T-1).

6.7.2.3. AF IC Authorizing Official and/or Delegated Authorizing Official is the approval authority for the use of standalone SCI computers within a TSWA. If the TSWA requestor plans to provide SCI processing via a standalone SCI computer, they submit a TSWA computer SOP, to their MAJCOM CISO and SSO along with their TSWA request (T-1).

**Figure 6.10. TSWA Standalone Computer SOP.****TEMPORARY SECURE WORKING AREA (TSWA) STANDALONE COMPUTER  
STANDARD OPERATING PROCEDURE (SOP)**

1. This document outlines the security procedures employed for use of a standalone computer within a Temporary Secure Working Area (TSWA). It applies to all personnel using the SCI computer within the TSWA. The computer is considered a Department of Defense (DoD) asset and national security interest computer system. Use of a DoD computer system is restricted to authorized users only. DoD computer systems will be monitored to ensure information security system integrity and the limitation of use to official purposes. The use of DoD computer systems constitutes consent to monitoring as an integral part of systems management. Information derived from system monitoring may be used as a basis for administrative, disciplinary or criminal proceedings. Use of a computer within the TSWA constitutes the staff member's understanding of all rules and procedures for use of the equipment as outlined below:
2. Any computer designated and approved use for within the TSWA (laptop or desktop) must be appropriately accredited and labeled (i.e., unclassified for NIPRNET, secret SIPRNET, and/or SCI for JWICS).
3. The computer configuration shall be checked to determine if:
  - a. All wireless capabilities has been disabled,
  - b. Network ports have been disabled (e.g., connections that would enable NIPRNET or SIPRNET connectivity),
  - c. The computer has had all current system updates/security patches/virus updates installed and completed,
  - d. Only approved, licensed software is installed.
4. The SCI computer shall receive system updates/security patches/virus updates via a JWICS connection only and within an accredited SCIF when not in use.
5. The computer will be stored within an accredited SCIF when not in use.
6. All media must be properly labeled and controlled by the media owner. Removable information storage media will have external labels clearly indicating the classification of the information and applicable associated markings (e.g., digraphs, tri-graphs). Examples include magnetic tape reels, cartridges, cassettes; removable media discs, disc cartridges, disc packs, diskettes, magnetic cards and electro-optical (e.g., CD) media. Labels will be affixed to all media in a manner that does not adversely affect operation of the equipment in which the media is used. Labels may be trimmed to fit the media. Labels for compact disks (CD) must not be placed on the CD itself, but on the CD container or envelope. Record the accounting number in the "control" block of the SF 71 1 and write the same number on the CD with a paint-pen, CD label maker or permanent marker. The number should not interfere with the operation of the CD.  
**Note:** Do not use pens that contain toluene.
7. The computer will be under constant escort/attendance by SCI indoctrinated individuals once taken from the host SCIF to the TSWA and returned. The computer shall never be left

unattended by SCI indoctrinated personnel.

8. A usage log for the SCI computer used within a TSWA shall be maintained. The log must reflect the dates the computer was taken/returned between the host SCIF (include the SCIF ID number) and a TSWA, the TSWA location, names of staff members performing the escorting of the equipment, their telephone numbers, and the TSWA points of contact/telephone numbers.
9. All classified media shall remain classified and controlled until explicitly declassified and/or destroyed I AW SCI destruction rules.

6.7.2.4. One-time use TSWA approval. The host MAJCOM SSO is the approval authority for a one-time use TSWA. TSWA approval of a conference room of similar location for one-time use does not require secret level control prior to the TSWA approval or after the TSWA termination. However, the facility is appropriately sanitized prior to and after the event. One-time use is classified as eight hours or less.

6.7.3. Temporary SCIFs (T-SCIFs). MAJCOM SSOs are the accreditation authority for T-SCIFs. When a T-SCIF is deployed in support of operations, the MAJCOM SSO may transfer the accreditation to the theater SSO and provide MAJCOM SSOs with information required by ICD 705 (T-1). All computer and network systems that process SCI is assessed and authorized for operation by AO/DAO. All T-SCIFs will be designated as controlled or restricted area (T-1).

6.7.4. MAJCOM SSOs will annually submit to AF CSA via email the following designations and delegations by 31 August (T-1). AF CSA submits to DIA/SEC in writing by 30 September annually.

6.7.4.1. Primary and Alternate MAJCOM SSO and MAJCOM SIO.

6.7.4.2. Accrediting Authority for T-SCIFs.

6.7.4.3. Accrediting Authority for TSWAs.

**6.8. Changes to Security Posture.** Within 24 hours, the MAJCOM SSO/CISO will report to AF/A2ZS (AF CSA) all changes affecting the security posture of any SCIF (T-1).

**6.9. Transfer of Security Cognizance.** When transferring the SCIF Physical and TEMPEST accreditations from one agency or MAJCOM to another, a minimum of 90 days before the transfer, all physical security standards will be maintained and accreditation records furnished to the gaining agency or MAJCOM for review (T-0). Upon review; gaining agency/MAJCOM may request waivers/exceptions for existing facility as deemed appropriate when submitting required updated accreditation package to DIA.

**6.10. Alarm System/Penetration/Security Response Testing.** SSOs and/or SSRs conduct alarm system, security response tests, and exercises semiannually; penetration exercises annually and will provide copies of the results to the local security forces per AFI 31-101. **Note:** Ensure advance coordination with a trusted agent at the security force prior to a scheduled test. SSOs/SSRs maintain a copy of the alarm system/security response force test record as prescribed by ICD 705 (T-0).

**Figure 6.11. Alarm System and Guard Response Test Log.**

Test date	Test Type	Individual Conducting Test	Equipment Tested			Malfunction		Corrective Action	Response Test		Comments
			BMS	Area	Tamper	Yes	No		Response Time	Name	

**6.11. Unclassified Speakerphones in a DIA Accredited SCIF.** The AF/A2 has delegated to MAJCOM SSOs the limited approval authority to activate unclassified speakerphones in SCIFs. MAJCOM SSOs may approve this activation only in DIA/SEC accredited SCIFs under their cognizance. MAJCOM SSOs are not authorized to delegate this approval any lower. The following security requirements apply.

6.11.1. Telephone will meet the technical security safeguards outlined in ICD 705 and be listed on the CNSSI 5006 (T-0).

6.11.2. Speakerphone approval is in support of a government requirement rather than out of convenience.

6.11.3. Telephone is located in a sole-use office or isolated area within a SCIF. All walls of the sole-use office or isolated area should meet sound transmission class (STC-50) to prevent the transmission of classified discussions taking place outside the office or isolated area. If the office or isolate area does not meet STC-50, procedures are implemented to ensure SCI discussions taking place in external areas adjacent to the sole-use office or isolated area are suspended to prevent the potential compromise of classified discussions via an active speakerphone.

6.11.4. If the approval is temporary (less than 24 hours) the related documentation is maintained as part of the permanent SCIF file.

6.11.5. Long-term or permanent approval of speakerphones are annotated in the fixed facility checklist (FFC). A copy of the FFC is forwarded to DIA/SEC for inclusion in the appropriate SCIF record and courtesy copied to AF CSA.

6.11.6. Telephones connected to classified networks are not included in this authorization.

## **6.12. Cellular Telephone Detectors.**

6.12.1. MAJCOM A2s are required to acquire cellular telephone detector devices for SCIFs that house more than 7 people and receive frequent (more than twice per week) visitors. These devices are placed at the entrance of all existing SCIFs meeting the above criteria by the end of FY 2017. Organizations will factor the cost of this device into all new construction, renovation, maintenance and sustainment of their Command's SCIFs (T-1).

6.12.2. MAJCOM A2s through the organization with a requirement may acquire any system that detects the most common cellular telephone signals in the 698 to 2690 MHz UHF frequency band. Two examples of such products are Cellbusters' Zone Protector™ and Berkley Varitronics Systems' Watchhound™ Cell Phone Security Monitor. These are provided as examples only and do not constitute endorsement or direction to purchase these two products.

6.12.3. SCI security officials emphasize the cellular phone security threat during regular security awareness, training, and education sessions and/or during recurring PED training (T-0).

6.12.4. SSO/SSR personnel will ensure that prescribed prohibited electronic items signage is prominently displayed outside of each SCIF (T-1).

### **6.13. VTC Systems.**

6.13.1. MAJCOM SSOs may approve the installation of VTC systems meeting the following configurations without seeking prior approval by DIA.

6.13.1.1. System operating at a single level.

6.13.1.2. Systems operating at multiple classification levels that employ an approved keyboard, video and monitor (KVM) switch.

6.13.2. VTC systems with prior approval, while not requiring prior approval by DIA; will be identify on the fixed facility checklist for the affected SCIF (T-0).

6.13.3. VTC system that operate at multiple classification levels and does NOT employ an approved KVM switch or switching device, i.e., audio-video (AV) mixers, AV system control units or AV extenders; will be approved by DIA certified TEMPEST technical authority (CTTA) prior to installation (T-0).

6.13.4. Installation of any VTC is IAW the TEMPEST accreditation for the SCIF and Red/Black separation requirements.

6.13.5. The SSO, in collaboration with the supporting site Information Assurance Security Manager, develops procedures to ensure potential vulnerabilities inherent with operating a VTC are addressed. Procedures will be incorporated into existing SCIF standard operating procedures (SOP) (T-0).

6.13.6. VTC rooms are constructed to achieve sound transmission standard (STC) 50.

**6.14. Badging Programs.** MAJCOM SSOs review the use of badging system(s) for spaces owned exclusively under their authority. AF CSA reviews all local badging system(s) that cross organizational lines of authority. AF CSA is the approval authority for the Intelligence Community Badge System (ICBS) whenever it is presented to the AF for use and access into AF owned SCIFs (T-1).

6.14.1. Authorizations for Special Access badging beyond the TS/SI/TK level needs to be validated by traditional clearance verification procedures in advance of the event or by validating clearances in JPAS or Scattered Castles, as defined by each IC element.

6.14.2. IC and local access badges are US Government property and shall be returned to the security office or issuing badge office upon transfer, separation, resignation, firing, termination of contract, and affiliation with the IC or no longer has a foreseeable need for access; the badge is retrieved and cancelled by the issuing IC element.

6.14.3. ICS 704-01 establishes requirements, processes, procedures, and responsibilities for the administration of the ICBS and the Intelligence Community Badge Interoperability Program (ICBIP). The ICBIP provides common badges that allow access to participating IC facilities and ensure positive identity verification with access audit capabilities.

6.14.3.1. AF communities who wish to participate in the ICBP submit a request to the AF CSA. The submittal includes organizational policies and procedures to implement the ICBS within their element. The request includes as a minimum:

6.14.3.1.1. Policies, SOP, EAP.

6.14.3.1.2. Procedures reviewed and approved through the MAJCOM SSO.

6.14.3.1.3. Availability of organization funds, to include equipment cost and installation.

6.14.3.1.4. Local computer element approvals.

6.14.3.2. IC badges do not display or include any insignia, other than the IC seal, to include a flag behind or within the individual's photo or any location on the front of the badge. The badge cannot display any element identifiers or contain any security overlays (SCI caveats) or smart chips.

**6.15. Control of Compromising Emanations (TEMPEST).** The TEMPEST accreditation message is the authoritative document identifying the requirements to contain compromising emanations within the inspectable space and is one of the three accreditations required for a SCIF to become operational with the other two being physical and information system accreditations. TEMPEST standards such as CNSSAM TEMPEST/1-13 and AFSSI 7702 reflects a risk management based approach to security. TEMPEST requirements are assessed on the threat, amount of inspectable space, equipment type, physical control, etc.

6.15.1. In addition to TEMPEST standards, there may be other installation standards to consider such as the National Electrical Code, local construction standards, and in particular NSA installation standards, which can be found at <http://it.org.nsa.ic.gov/procmgmt/standards>. Failure to follow these standards can result in significant delays, additional costs, and possible denial of services.

6.15.1.1. TEMPEST accreditation documentation is processed through the MAJCOM SSO to the respective accrediting authority with a copy sent to AF/A2-CSA (T-1).

6.15.1.2. For SCI facilities, the accrediting authority (typically DIA or NSA) provides the organization a TEMPEST accreditation message or letter identifying their inspectable space and TEMPEST countermeasure requirements including any applicable RED/BLACK separation as described in CNSSAM TEMPEST/1-13. Information on the SCIF accreditation process can be found in ICD 705, 705-1, ICS 705-2. Information on the DIA accreditation process can be found in DoD Manual 5105.21, Volumes 1 through 3 or by calling DIA/SEC-1B. Information on the NSA process is available through NSA/I3332.

6.15.2. Request a TEMPEST reaccreditation when a major modification of the facility occurs or the TEMPEST profile of the facility changes as described in DoD Manual 5105.21, Vol 2. A major modification is anything that changes or negates a TEMPEST countermeasure. A change in the TEMPEST profile is anything that alters the inspectable space, the level of TEMPEST threat, or the technology used to electronically process the SCI. Requests are documented on the TEMPEST Checklist (ICD/ICS 705) and submitted to the accrediting authority through SSO channels.

6.15.3. The RED/BLACK facility design philosophy is to provide sufficient attenuation or isolation between RED equipment/lines and BLACK equipment/lines that leave the inspectable space. The level of attenuation or isolation is dependent on the size of the inspectable space. The CNSSAM TEMPEST/1-13 RED/BLACK requirement levels (e.g., I, II, III) correspond to the level of protection needed to contain compromising emanations within the inspectable space. The levels are based upon the installation of Commercial-Off-The-Shelf (COTS) equipment within a standard commercially built office building. As a part of risk management, the requirement level is less stringent for lower classification levels of information processed within the US and is more stringent for higher classification levels of information processed outside the US.

6.15.4. Facility Shielding and Shielded Enclosures. The use of shielded enclosures and alternative shielding materials is based on the results of an evaluation performed according to CNSSI 7000. The evaluation is conducted or validated by the cognizant CTTA.

6.15.5. Windows are one of the most vulnerable aspects of a facility. Numerous window treatment products have been developed to provide differing degrees of attenuation to various forms of wireless transmissions such as radio frequency and infrared. The TEMPEST accreditation provided by the cognizant CTTA identifies if window treatments are required. The installation of window blast protection measures provides an excellent opportunity to also add wireless attenuation measures with minimal additional cost.

6.15.6. Wireless, especially Radio Frequency (RF), devices and systems pose a particularly significant TEMPEST hazard if not installed using good engineering practices. Devices that fall under this category are radio transmitters, receivers, land mobile radios, receive and transmit pagers, cellular telephones, wireless microphones, cordless telephones, portable data assistants, wireless local area networks, etc. These devices are generally prohibited in a SCIF.

6.15.6.1. IC Tech Spec for ICD and ICS 705 places wireless devices into high, medium, and low vulnerability categories and provides initial guidance for their use. Receive-only pagers and infrared devices that convey no intelligence data (text, audio, video, etc.) such as mice, remote controls and pointing devices pose no TEMPEST risk and require no TEMPEST mitigation to be introduced into SCIFs.

6.15.6.2. The installation of wireless devices and RF transmitters in spaces that process NSI presents other information assurance vulnerabilities and will require additional approval from the AF CSA (T-1). Coordination with local security officials and approval through the MAJCOM SSO is required prior to introducing wireless devices into a SCIF.

6.15.7. TEMPEST in the Airborne Environment (Tactical Equipment). See CNSSAM TEMPEST/1-13 and IC Tech Spec for ICD and ICS 705, for unique aircraft operations and installation. Based on AFSSI 7702, all aircraft carrying classified processing systems are tested according to CNSSAM TEMPEST/01-02 during airborne system procurements and modifications unless otherwise specified by a CTTA. This includes remotely piloted aircraft.

## CHAPTER 7

### VISITOR CONTROL

**7.1. Overview.** The SSO and the CSSO are the official channels and points of contact for verification of SCI accesses through JPAS and Scattered Castle. The AF clearance verification is a “pulled” not “pushed” process using the information in JPAS or Scattered Castles.

7.1.1. JPAS is the primary DoD clearance verification system.

7.1.2. Scattered Castle is the secondary system through the IC Security Clearance Repository for verification of clearances and accesses.

7.1.3. Local listing(s) though highly discouraged can be used for access control by the SSO or CSSO and will be approved by the local SIO (T-1). Procedures will include 100% verification by the SSO or designated authorities using the DoD primary source JPAS.

**7.2. JPAS or Scattered Control.** JPAS and Scattered Castles when used to verify personnel security clearances does eliminate the need for visit and permanent certification (Perm-Cert) except for special circumstances, i.e. large scale exercises. However, special circumstances will require the approval of the AF CSA (T-1).

**(Note:** If the local procedures of the visited agency require a visitor or permanent certification prior to access, send the requested information. Accomplishing the mission is the number one priority.)

7.2.1. SSOs accept, from other AF units and IC agencies, all “in-scope”, security clearance, or access determinations unless there are waivers, conditions, or deviations. Individuals with records where there are waivers, conditions, or deviations; SSOs contact the owning SSO and request additional information before allowing access (T-0).

7.2.2. The organization disclosing the classified information has the responsibility to establish the positive identification of all individuals before determining the need-to-know or need-for-access; prior to disclosing any classified information or granting access. The government sponsor (military or civilian) within the visited organization coordinates with the security office prior to the visit to ensure the visitor has the appropriate clearance prior to access (T-2).

7.2.3. In the case of contractors, the COR for the specific contract provides a list of contractor personnel, copies of the DD Form 254 with attachments, and the exercised period of performance dates of the contract being worked within the visited SCIF to the unit sponsor and/or SSO per local procedures (T-2).

7.2.4. Visitors are still required to coordinate with the sponsoring organization to ensure access and badging requirements are completed.

7.2.4.1. For visits longer than 15 calendar days, the SSO with security cognizance over the visited unit will in-processes the visitor and claim “servicing” responsibility in JPAS (T-1). This ensures notifications regarding the visitor’s security clearance are received. Visits less than 15 calendar days, the SSO with security cognizance over the visited unit may claim “servicing” responsibility in JPAS after prior coordination with the visitor’s SSO.

7.2.4.2. When reviewing JPAS for SCI access for visiting personnel, the lack of a government SCI Security Management Office (SMO) code, or “US” access could be considered errors in the currency of JPAS data. When encountering these situations, security officials notifies the sponsor and inform the visitors to have their SSO update the relationship status and/or US accesses in JPAS (T-2).

7.2.5. SSO access certification via JPAS, message or facsimile is still authorized if:

7.2.5.1. JPAS and/or Scattered Castles record does not validate the level of access required.

7.2.5.2. JPAS and/or Scattered Castles record does not accurately reflect visitor’s affiliation.

7.2.5.3. Requested for contractors owned by one MAJCOM and permanently working in another MAJCOM’s SCIF. The owning SSO and the host SSO work together to ensure needed information is obtained.

7.2.5.4. The clearance certification message serves some additional purpose such as access to restricted databases.

**7.3. Visits to Foreign-Owned Facilities.** MAJCOM SSOs are responsible for recertifying SCI accesses of their command’s military, DoD civilian and contractors visiting foreign SCIFs. Traveler’s coordination with Foreign Disclosure Office (FDO) is also required (T-1).

#### **7.4. Visits By Foreign Nationals.**

7.4.1. MAJCOM SSO are required to certify the SCI access of foreign nationals authorized to visit their command’s SCIFs (T-1).

7.4.2. FDO Approval. Coordination with and visit approval by the supporting FDO is also required. Submit the request to the FDO at least 30 days in advance of the visit (T-1).

7.4.3. Component commands are authorized to verify through their combatant command foreign national access for AF SCIFs in their AOR (T-1).

**7.5. Escorts.** General procedures are outlined in DoDM 5105.21-V2, Enclosure 3, Paragraph 9.

7.5.1. A flashing or rotating light is recommended, to the maximum extent possible, to indicate the continued presence of non-SCI-indoctrinated personnel in the SCIF.

7.5.2. Waivers to escort policy and procedures may be granted by the SIO on a case-by-case basis in writing.

#### **7.6. Contractor Special Security Officers (CSSO).**

7.6.1. AF Visits to Contractor Facilities. SSOs are authorized to certify SCI accesses of AF and contractor personnel directly to a CSSO.

7.6.2. Records Requirements. CSSOs retain a record of access certifications for the duration of the visit or permanent certification. SSO will maintain current written validation of CSSO and alternates appointments prior to accepting contractor access certification (T-2).

## CHAPTER 8

### INDUSTRIAL SECURITY

**8.1. Overview.** This chapter provides security guidance for the AF and their associated contractors. Also included is guidance for the positions: CORs, CSSOs, FSOs, and organizations that possess SCI contracts.

**8.2. Facility Security Clearance (FCL) Requirements for Access to SCI.** Contractors must have a Final Top Secret FCL prior to having access to SCI (T-0).

**8.3. Contractor/Consultant Security.** The SIO or designees may grant SCI access to US contractor employees under the following conditions:

8.3.1. The DD Form 254 certifies SCI is required in the performance of the specified task (Item 10e(1) and (2) marked “Yes”) to which the individual has been hired.

8.3.2. The DD Form 254 is annotated with the Addendum of SCI clauses. Refer to Figure 8.1, *DD Form 254, SCI Addendum*.

**Figure 8.1. DD Form 254 SCI Addendum.**

<b>SCI ADDENDUM</b>
<p>1. <b>Reference Block 14:</b> This contract requires access to Sensitive Compartmented Information (SCI). Per (list applicable DoD publications, ICDs, DCIDs, DoDM 5105.21, Volumes 1,2 3 and AFMAN 14-401, Joint DoDISS Cryptologic SCI Information Systems Standards (JDCSISSS), NISPOM Supplement, etc.) provides the necessary guidance for physical, personnel, information and information systems security measures and is part of the SCI security specifications for the contract.</p> <p>2. Name, organization, telephone number and address of the Contract Officer Representative (COR) for the SCI portion of this contract is:</p> <p><b>Name Office Symbol Phone</b></p> <p>3. All DD Form 254s prepared for subcontracts involving access to SCI under this contract must be forwarded to the COR for approval and then to (SSO, location) for review and concurrence prior to award of the subcontract. Inquiries pertaining to classification guidance on SCI will be directed to the COR listed in para. 2 above. SCI security management issues shall be directed to (SSO, office symbol, location, local and DSN telephone numbers).</p> <p>4. SCI access is subject to U.S. Government review and approval as outlined in the aforementioned SCI security guidance. Upon completion or cancellation of the contract, the SSO/CSSO will debrief all personnel not required for contract closeout and those positions will be disestablished.</p> <p>5. Names of contractor personnel requiring access to SCI and justification for SCI access will be submitted for coordination and action to (SSO, location) after the COR’s approval/concurrence. Upon receipt of written approval from the COR, the Facility Security Officer (FSO) and/or Contractor Special Security Officer (CSSO) may submit the necessary forms to the Defense Security Service (DSS) for a Single Scope Background Investigation (SSBI) for those personnel nominated for SCI in accordance with the National Industrial Security Program Operating Manual (NISPOM).</p> <p>6. The SSO/CSSO can grant access to only those who possess the necessary security clearance and who are actually providing services under the contract. Further dissemination to other contractors, sub-contractors, other government agencies, private individuals or organizations is prohibited unless authorized in writing by the releasing agency.</p> <p>7. SCI materials furnished in support of this contract remains the property of the DoD department or command that released it. Upon completion or cancellation of the contract, all SCI materials furnished will be returned to the direct custody of the originator of the materials.</p>

8. Classified foreign intelligence materials must not be released to foreign nationals or immigrant aliens whether or not they are also consultants, U.S. contractors, or employees of the contractor regardless of the level of their security clearance, except with advance written permission from the originator.
9. Contractor personnel must maintain accountability for all intelligence (to include foreign intelligence) materials released to their custody.
10. Contractor personnel must not reproduce classified foreign intelligence without advance approval of the releasing agency. If permission is granted, each copy will be controlled in the same manner as the original. The CSSO must not destroy any classified foreign intelligence without advance approval of the releasing agency.
11. A SCIF meeting the physical security requirements in DCID 6/9 or ICD 705 is required for this contracting effort. All SCI used for this contract shall be stored, handled, and maintained in an accredited SCIF, be it the local contractor SCIF or similarly SCI accredited facilities used by the contractor. Address of the SCIF for contract execution:
- 11.1. (Office Symbol and Company Name, street address, Bldg #, City, State, and Zip Code.
- 11.2. SCIF ID Number.
- 11.3. Name and Telephone number of FSO/CSSO.
12. Visits. The contractor will submit the written request for SCI visit certifications through the COR for approval of the visit. The certification must arrive at their servicing (SSO name) at least three working days prior to the visit.
13. Information assurance and electronic processing; information security (computer) and network connectivity require accreditation of the equipment connectivity.
14. **Reference Block 15.** This contract requires access to SCI. If the contractor has established a SCIF, DIA and its designees are responsible for all inspections of the contractor SCIF and SCI security management program for ensuring compliance with all SCI security regulations and policies. If a new SCIF must be established in accordance with this contracting effort, permission to build/accredit a SCIF must be requested through the COR and forwarded to the SSO. Special Security Officers reserve the right to conduct program reviews of AF SCI materials and SCI program management to ensure the protection of AF equities.
15. Contract estimated completion date: (DATE)
- (**Note:** Section "F" of the contract usually provides the Period of Performance. Option years are not to be included as an option is not valid until exercised by the government. Minor modification are authorized.)

8.3.3. The local unit is listed as a performance location on the DD Form 254 (Block 8).

8.3.4. The local COR endorses the requirement. If the COR is not located on the base a local government representative is appointed (Names are annotated in block 13). The COR must be indoctrinated for SCI access in order to verify the SCI contract deliverables (T-1). The COR is also read into any program material to hold accountability of released intelligence. CORs not verifying SCI deliverables are not to be granted SCI access.

8.3.5. The individual's ICD 704 eligibility is favorably adjudicated. If not adjudicated, the SSO annotates SCI SMO ownership of the individual in JPAS, requests an upgrade of eligibility through the DoD CAF and waits for the case to be adjudicated.

8.3.6. The individual has signed a NdS.

8.3.7. A SCI security indoctrination has been completed.

**8.4. DD Form 254 Preparation.** MAJCOM SSOs are responsible for SCI security on any contract requiring access to SCI in a facility under their cognizance. MAJCOM SSO, may give approval (in writing) for specific instances where the Supporting/Serviceing SSO/SSR signs the DD Form 254. When the Supporting/Serviceing SSO/SSR has cognizance over a contract a copy of the final DD Form 254 is sent to the MAJCOM SSO (T-1).

8.4.1. MAJCOM SSOs identify supporting security officials who shall provide minimum SCI requirements to the COR as a DD Form 254 addendum when a contract or solicitation is being prepared. Refer to Figure 8.1 for minimum requirements. MAJCOMs may supplement as needed (T-2).

8.4.2. Access to SCI will be fully justified in the SOW or PWS to include the specific types of information needed, whether access to JWICS is needed, why sanitized intelligence cannot be utilized, and the impact if access is not approved (T-1). Granting SCI access for the purpose of allowing a contractor to transit an SCI area in route to a work site or for convenience of assigned personnel is not sufficient justification for approving access.

8.4.3. Local SSO/SSR forward the DD form 254 and associated SCI Addendum to the SIO or designated representative for the final review for contractor access before MAJCOM approval (T-1).

### **8.5. Subcontractors.**

8.5.1. The prime contractor is responsible for preparing DD Form 254s for SCI access of their subcontractors. Completed subcontractor DD 254's are provided to the supporting SSO for their review and validation. Supporting SSO submit the reviewed and validated DD Form 254 to the MAJCOM SSO (listed on the Prime Contract) for approval (T-1).

8.5.2. Subcontractor employees will meet all security requirements prior to access (T-1).

### **8.6. Contracts Affecting other MAJCOMs/Bases.**

8.6.1. When a contract requires work at a base, for more than 30 days, other than where it was let, the SSO responsible for the work location receive a copy of the DD Form 254 and associated addendums prepared by the COR responsible for the contract. A DD Form 254 which affects other MAJCOMs/bases should include a requirement stating the contractor complies with all local security requirements at the work location (T-1).

8.6.2. The SSO with security cognizance at the work location is authorized to issue a supplemental SCI addendum covering local situations/requirements.

### **8.7. Contractor Visit Authorizations.**

8.7.1. A contractor is not authorized access to classified information at any level unless authorized by a DD Form 254 for their contract.

8.7.2. If a contractor needs to visit an AF installation or activity, the visit is coordinated in advance with the host installation and host agency. The installation commander is the sole authority responsible for granting contractors access to the installation, regardless of which DOD agency, military service component, or activity awarded the contract. The installation commander designates contractors who require access to the installation in the performance of a government contract as intermittent visitors, integrated visitor groups, or cleared facilities (T-1).

8.7.3. If a contractor's visit requires access to SCI, the visited location verifies the visitor's security clearance and SCI access levels. Verification of a visitor's clearance may be accomplished by a review of JPAS or Scattered Castles databases. Verification that the visit is in support of performance under a valid classified contract is also required and may be accomplished by a review of the relevant DD Form 254 or certification from the COR

responsible for the contract. The COR provides certification, contractor's name, address, and telephone number, assigned Commercial and Government Entity (CAGE) code, if applicable, and certification of the level of the facility security clearance is required (T-1).

**8.8. SSO Record Keeping Requirements for Contractors.** SSOs maintain current DD Form 254s, COR appointment letters from the contracting office, COR duties letter, and a list of contractors working the specific contract (validated by COR on an annual basis or when changes are made). Records are maintained for two years after the contract is terminated, performance has ended or the contract is closed out (T-2).

**8.9. Release of Intelligence to US Contractors.**

8.9.1. AF/A2 implements and carries out the DNI's policies and procedures for using, protecting and disseminating intelligence. AF/A2 is the AF's final authority for approving the release of intelligence to contractors. Only AF/A2 can release information to contractors from the National Intelligence Analytical Memoranda without identifying it as national intelligence.

8.9.2. The MAJCOM SIO and their field command designees can release intelligence to their command contractors without specific approval from the AF/A2 if the intelligence meets the criteria listed in, ICD 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information*, intelligence is not marked with restricted control markings, and the intelligence is not restricted to the executive branch of the US Government. For access the SIO or designee will perform the following functions:

8.9.2.1. Evaluate the sponsor's request for intelligence by examining the DD Form 254, and SOW or PWS to determine if the specific intelligence is appropriate for the contract. Ensure network access provided to contractor(s) (e.g. access to Secure Internet Protocol Network [SIPRNET], JWICS, and/or any other classified network) for the purpose of contract execution is documented on the DD Form 254 in Block 11. The finalized DD Form 254 is used by the SIO or designee appointee to document the release of intelligence information to the contractor (T-1).

8.9.2.2. Ensure the COR accounts for all intelligence information released to the contractor (T-1).

8.9.2.3. Ensure electronic access to classified information is documented via the DD Form 254 and is accounted for by using government oversight (T-1).

8.9.2.4. Ensure Air Staff activities, MAJCOMs, and FOAs without an SIO refer requests to the AF CSA for release approval.

8.9.3. Intelligence that carries the PROPIN markings requires written permission of the originating agency before release to contractors within or outside of government owned or controlled facilities.

8.9.4. Intelligence that carries the ORCON marking requires written permission of the originating agency before release to a contractor outside of government owned or controlled facilities. Sponsoring agencies delete any reference to the Central Intelligence Agency (CIA) phrase "Directorate of Operations" and any of its components, place acquired, field number, source description, and field dissemination from all CIA Directorate of Operations reports passed to contractors, unless prior approval to do otherwise is obtained from CIA. (T-0)

8.9.5. If you cannot sanitize the documents, you can request release for intelligence bearing these markings through the originator. Provide a courtesy copy of the request to your MAJCOM SSO (T-1).

8.9.6. All inquiries concerning source, acquisition, use, control or restrictions pertaining to Intelligence Information are directed to the releasing agency (T-1).

8.9.7. Classified foreign intelligence materials must not be released to foreign nationals or immigrant aliens whether or not they are also consultants, US contractors, or employees of the contractor, regardless of the level of their security clearance, except with advanced written permission from the originator (T-1).

8.9.8. The contractor will be trained and authorized by the SIO/SSO to courier SCI documents, material, or equipment if required by the DD Form 254 (T-1).

**8.10. Foreign Ownership, Control, or Influence (FOCI).** A US company is considered to be under FOCI whenever a foreign interest has the power, direct or indirect (whether or not exercised and whether or not exercisable through the ownership of the US company's securities, by contractual arrangements or other means), to direct or decide matters affecting the management or operations of the company in a manner that may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

8.10.1. If a government contracting activity (GCA) requires a company cleared under a Special Security Agreement (SSA) to have access to SCI, the GCA is required to complete a National Interest Determination (NID) to confirm that disclosure of such information will not harm the national security interests of the US (T-0).

8.10.2. All NIDs for SCI access is processed by the Office of the Director of National Intelligence (ODNI) or the Office of the National Counter Intelligence Executive (ONCIX), Special Security Directorate (SSD). ONCIX/SSD should complete the SCI NID process within five to thirty calendar days (T-1).

8.10.3. The requirement for NIDs applies equally to new contracts to be issued to companies already cleared under SSAs or proxy agreements as well as existing contracts when cleared companies are acquired by foreign interests and an SSA or proxy agreement is the proposed mitigation. NIDs may be program, project or contract-specific.

8.10.4. If foreign interests can or may be able to control or influence the operations or management of a contractor organization, that contractor organization is under FOCI. Contractor organizations under FOCI are generally ineligible for access to SCI and SCI activities.

8.10.5. Waivers to Ineligibility. The ODNI may support a NID to waive the ineligibility for access of a contractor organization if a review of the circumstances shows a need to grant access, and it can be determined that:

8.10.5.1. The FOCI does not involve communist countries or countries overtly hostile to the US.

8.10.5.2. Indebtedness to foreign interests does not exceed five percent of the organization's current assets.

8.10.5.3. Information disclosed regarding securities held in “nominee shares” or “street names” reveals no indication of adverse FOCI.

8.10.5.4. Foreign interest does not have the right to control or influence the election, appointment, or tenure of an organization’s managing officials.

8.10.6. The ODNI approves waivers based on an approved SSA or proxy agreement. The waiver is contingent on an annual review of the company’s eligibility for continued SCI access to ensure the organization continues to have measures in place that preclude foreign interests from gaining access to SCI.

8.10.6.1. The annual facility program review, including a review of the SSA or proxy agreement, performed by the Defense Security Service (DSS) can fulfill this requirement. DSS certifies a favorable review to the appropriate COR and servicing SSO.

8.10.6.2. More frequent reviews of an organization’s eligibility for continued SCI access may be required if changes occur that could enable foreign interests to control or influence the management of operations of the organization to the extent that it would endanger the security of SCI or SCI activities.

8.10.6.3. When there is doubt about an organization’s eligibility and willingness to safeguard SCI against foreign access; in the interest of national security, access authorization will be revoked.

8.10.7. Email correspondence is the only accepted means of submitting a National Interest Determination (NID) request to the ODNI. The request will not be processed unless it includes the following information: (T-0).

**Figure 8.2. National Interest Determination Request.**

<b>NID REQUEST</b>	
1.	A copy of the SSA or reasons why SSA cannot be released.
2.	Proposed contractor and/or subcontractor to include:
	Contractor’s Name and Address
	Cage Code
	Description of its Foreign Ownership
	Prime Contract Number, Subcontract Number and Solicitation Number
	Whether the proposed contract is part of an existing program or project
3.	General description of the procurement and performance requirements that include the following:
	Why the foreign company needs access to SCI
	Who will have access to the material
4.	List the national security interests involved and the ways in which the release of information is consistent with those national interests
5.	Existing internal agency threat assessments regarding the contractor or subcontractor. If threat assessment does not exist, DSS completes the requirement during the DSS review process within their organization.
6.	A copy of the last DSS annual Facility Program Review (conducted within the last year).

8.10.8. If the MAJCOM SSO receives the NID, the MAJCOM SSO forwards the SCI portion of the NID request to the AF CSA electronically to [usaf.pentagon.af.a2.mbx.af-A2ZS-workflow@mail.mil](mailto:usaf.pentagon.af.a2.mbx.af-A2ZS-workflow@mail.mil).

8.10.9. Organization Eligibility and Changes. Notify AF CSA immediately of any changes to the organization's security posture that could affect the organization's eligibility and willingness to safeguard SCI against foreign access, or if DSS revokes the FCL (T-1).

## CHAPTER 9

### SECURITY EDUCATION TRAINING AND AWARENESS PROGRAM (SETA)

**9.1. Overview.** How well an employee understands their responsibilities should be the focal point of any security program when it comes to protecting our nation's secrets. Employees at every level, are educated in and frequently reminded of sound security practices and procedures. SETA is the process through which employees are made aware of the threats to, and critical safeguarding procedures of National Security Information, including SCI. Upon appointment, designated SCI Security Officials, SSO, SSRs, CSSOs and specified support personnel should attend a SCI Security Officials Course provided by ODNI or DoD, (a similar course may be substituted) within 6 months upon assumption of these duties. If the appointees cannot attend training within 6 months SSO, SSR or SIO conducts training locally designed to/for the duties assigned (T-2).

**9.2. SCI Security Education Program.** Each SSO/CSSO ensures all SCI indoctrinated personnel under his or her security cognizance receives security awareness information at least annually (T-2). Security training must be of sufficient frequency and visibility to identify SCI as requiring special and unique protection. It is highly suggested to develop quarterly training with in person classes.

9.2.1. Identify the roles and responsibilities of the SIO, SSO, and other appropriate officials, emphasizing individual responsibilities regarding the protection, use, and dissemination of SCI and need to adhere to SCI eligibility standards.

9.2.2. Place special emphasis on recent or recurring SCI security incidents or problems as well as local SCI security policies and procedures. The SSO may use a variety of transmission means (newsletters, security bulletins, pamphlets, seminars, and posters), at appropriate classification levels (T-2).

9.2.3. The Security Education Program follows training outlined in DoDM 5105.21-V3, and DNI required training on Unauthorized Disclosures and ORCON.

9.2.4. Specialized Education and Training. SIO/SSOs ensure SCI courier policies, procedures, and responsibilities are given to individuals designated by the SIO/SSO to act as an SCI courier (T-1).

9.2.5. In developing local SCI security educational and training programs, use any applicable regulation, current security trends and lessons learned from security incidents investigations.

9.2.5.1. Maintain SETA records of SCI education and training for 2 years (T-1).

9.2.5.2. Derivative security classification training must be completed within 30 days of arrival at a new duty station/assignment and once every two years thereafter. Individuals that fail to complete either the initial training within 30 days or fail to complete the biennial training at least once every two years are considered "non-current" and no longer have authority to prepare classified documents to include classified emails regardless of system. (T-0).

**9.3. Education and Training Responsibilities.**

9.3.1. AF CSA. Manage and evaluate the USAF SCI SETA program to include production and distribution of standard IC SCI indoctrination briefing and debriefing materials as well as continuing and specialized security training materials.

9.3.1.1. Publish electronic SCI security advisories. ROXAD is a DAG used to disseminate security education and awareness information to the field. ODANS is a DAG used to disseminate SCI policy and guidance to all USAF SSOs.

9.3.1.2. Conduct periodic AF SCI Security Officials' conferences, workshops and other SCI security-related forums, as required.

9.3.2. SIO. Provide adequate resources to support the SSO's SCI security education and training program (T-2).

9.3.3. SSO/CSSO will develop and implement an SSO proficiency training program (T-2). Training briefs will cover topics outlined in DoDM 5105.21-V3 as a minimum (T-1)

9.3.3.1. Manage, conduct, and evaluate local and subordinate SCI security education and training (T-2).

9.3.3.2. Ensure all SCI indoctrinations, re-indoctrinations, foreign travel briefings, SCI debriefings and local security orientation briefings are conducted (T-2).

9.3.3.3. Conduct annual SCI security awareness training (T-2).

9.3.3.4. Ensure non-SCI base support staffs (e.g., medical, fire, security forces, contract officers, public affairs, legal, etc.) are aware of their need to support the SCI management program (T-2).

9.3.3.5. Provide a local SCI security orientation briefing to all newly assigned SCI-indoctrinated personnel within 30 days of arrival. (This briefing may be presented at the time of indoctrination/re-indoctrination and may also be used to meet the annual requirements (T-2).

9.3.3.6. Ensure all SCI indoctrinated personnel complete the mandatory DNI Unauthorized Disclosure Training and Awareness Course within 30 days of assignment and annually thereafter. Training can be located at [www.ncix.gov/training/wbt.php](http://www.ncix.gov/training/wbt.php) or on JWICS at [www.ncix.ic.gov/training/wbt.html](http://www.ncix.ic.gov/training/wbt.html). In addition, Defense Security Service offers the course and it may be reached on NIPR at <http://www.cdse.edu/catalog/information-security.html>. Locally developed training is authorized with written approval from the AF CSA (T-1).

9.3.3.6.1. Report the completion of training, by percentage of personnel trained, by 15 January to your MAJCOM SSO (T-2).

9.3.3.6.2. MAJCOM SSOs report the percentage of all MAJCOM personnel trained by 15 February to AF/A2ZS.

VERALINN JAMIESON, Maj Gen, USAF  
Deputy Chief of Staff, Intelligence,  
Surveillance, and Reconnaissance

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

- AFI 16-1404, *Air Force Information Security Program*, 29 May 2015
- AFI 31-406, *Applying NATO Protection Standards*, 29 July 2009
- AFI 31-101, *Integrated Defense*, 8 October 2009
- AFI 31-501, *Personnel Security Program Management*, 27 January 2005
- AFI 33-324, *The Air Force Information Collections and Reports Management Program*, 6 March 2013
- AFI 33-360, *Publications and Forms Management*, 1 December 2015
- AFI 35-102, *Security and Policy Review Process*, 4 May 2016
- AFI 36-2608, *Military Personnel Records System*, 26 October 2015
- AFI 36-2911, *Desertion and Unauthorized Absence*, 15 October 2009
- AFMAN 33-363, *Management of Records*, 1 March 2008
- AFPD 14-3, *Control, Protection, and Dissemination of Intelligence Information*, 1 May 1998
- CNSSI 7000, *TEMPEST Countermeasures for Facilities (C)*, May 2004
- DoD 5200.2-R, *DoD Personnel Security Program, January 1987*
- DoDM 5105.21, Volume 1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security*, October 19, 2012
- DoDM 5105.21, Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security*, October 19, 2012
- DoDM 5105.21, Volume 3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security and Special Activities*, October 19, 2012
- HAF Mission Directive 1-33, *Deputy Chief of Staff of the Air Force, Intelligence, Surveillance & Reconnaissance*, 18 September 2015
- ICD 703, *Protection of Classification National Intelligence, Including Sensitive Compartmented Information*, 21 June 2013
- ICD 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to SCI*, 1 October 2008
- ICD 705, *Sensitive Compartmented Information Facilities*, 26 May 2010
- ICD 710, *Classification and Control Markings System*, 21 June 2013
- ICS 705-2, *Standards for the Accreditation and reciprocal Use of Sensitive Compartmented Information Facilities*, 11 February 2013.

ICPG 704.1, *Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*, 2 October 2008

ICPG 710.1, *Application of Dissemination Controls: Originator Control (ORCON)*, 25 July 25 2012

Intelligence Community Policy Memorandum 2007-700-3, *Director of National Intelligence Foreign Travel Reporting Form*, 13 September 2007

IC Tech Spec *Technical Specifications for Construction and Management of Sensitive Compartmented Facilities, Version 1.3*, 10 September 2015

### ***Adopted Forms***

AF Form 847, *Recommendation for Change of Publication*

DD Form 254, *Contract Security Classification Specifications*

DD Form 1847-1, *Sensitive Compartmented Information Nondisclosure Statements (NdS)*

IC Form 4414, *Sensitive Compartmented Information (SCI) NdA*

### ***Abbreviations and Acronyms***

**ACCM**—Alternative or Compensatory Control Measures

**AD**—Active Duty

**ACC**—Air Combat Command

**AETC**—Air Education and Training Command

**AF/A2**—Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance

**AFGSC**—Air Force Global Strike Command

**AFI**—Air Force Instruction

**AFMAN**—Air Force Manual

**AFMC**—Air Force Material Command

**AFOSI**—Air Force Office of Special Investigations

**AFOTEC**—Air Force Operational Test and Evaluation Center

**AFPD**—Air Force Policy Directive

**AFDW**—Air Force District of Washington

**AFR**—Air Force Reserve

**AFRC**—Air Force Reserve Command

**AFSC**—Air Force Specialty Code

**AFSOC**—Air Force Special Operations Command

**AFSPC**—Air Force Space Command

**AFVA**—Air Force Visual Aid  
**ANG**—Air National Guard  
**AO**—Authorizing Official  
**AUTODIN**—Automatic Digital Network  
**CAB**—Compartmented Address Book  
**CAF**—Central Adjudication Facility  
**CAGE**—Commercial and Government Entity  
**CAPCO**—Controlled Access Program Coordination Office  
**CIA**—Central Intelligence Agency  
**COI**—Community of Interest  
**COMINT**—Communications Intelligence  
**COMSEC**—Communications Security  
**CONOPS**—Concept of Operations  
**COR**—Contracting Officer's Representative  
**CSA**—Cognizant Security Authority  
**CSAF**—Chief of Staff of the Air Force  
**CSSO**—Contractor Special Security Officer  
**CTTA**—Certified TEMPEST Technical Authority  
**CUA**—Co-Utilization Agreement  
**DA&M**—Director of Administration & Management  
**DAF**—Department of the Air Force  
**DAG**—DSSCS Address Group  
**DAO**—Delegated Authorizing Official  
**DCI**—Director of Central Intelligence  
**DCID**—Director of Central Intelligence Directive  
**DCS**—Deputy Chief of Staff  
**DD Form**—Department of Defense Form  
**DIA**—Defense Intelligence Agency  
**DIA/SEC**—DIA Counterintelligence and Security Activity  
**DIRNSA**—Director, National Security Agency  
**DISA**—Defense Information Systems Agency  
**DNI**—Director of National Intelligence

**DoD**—Department of Defense  
**DoD CAF**—Department of Defense Consolidated Adjudication Facility  
**DoDIIS**—Department of Defense Intelligence Information System  
**DRU**—Direct Reporting Unit  
**DSN**—Defense Switches Network  
**DSS**—Defense Security Service  
**DSSCS**—Defense Special Security Communication System  
**DTG**—Date-Time-Group  
**EAP**—Emergency Action Plan  
**EO**—Executive Order  
**FCL**—Facility Clearance  
**FDO**—Foreign Disclosure Officer  
**FFC**—Fixed Facility Checklist  
**FOA**—Field Operation Agency  
**FOCI**—Foreign Ownership, Control, or Influence  
**FOUO**—For Official Use Only  
**FSO**—Facility Security Officer  
**FY**—Fiscal Year  
**G**—GAMMA  
**GCA**—government contracting activity  
**GCO**—GAMMA Control Officer  
**GENSER**—General Service  
**HCS**—Human Intelligence (HUMINT) Control System  
**HICE**—Head of the Intelligence Community Element  
**HUMINT**—Human Intelligence  
**IA**—Information Assurance  
**IAW**—In Accordance With  
**IC**—Intelligence Community  
**ICD**—Intelligence Community Directive  
**ICPG**—Intelligence Community Policy Guidance  
**ICS**—Intelligence Community Standard  
**ICSCR**—Intelligence Community Security Clearance Repository

**IG**—Inspector General  
**INFOSEC**—Information Security  
**IPA**—Intergovernmental Personnel Act  
**IS**—Information System  
**ISR**—Intelligence, Surveillance, and Reconnaissance  
**ISSO**—Information System Security Officer  
**ISSM**—Information System Security Manager  
**IT**—Information Technology  
**JPAS**—Joint Personnel Adjudication System  
**JWICS**—Joint Worldwide Intelligence Communications System  
**KCS**—Klondike Control System  
**MAJCOM**—Major Command  
**MOA**—Memorandum of Agreement  
**NAC**—National Agency Check  
**NACS**—National Agency Check/National Agency Check  
**NASIC**—National Air and Space Intelligence Center  
**NATO**—North American Treaty Organization  
**NDA**—Nondisclosure Agreement  
**NdS**—Nondisclosure Statement  
**NGA**—National Geospatial-Intelligence Agency  
**NID**—National Interest Determination  
**NISP**—National Industrial Security Program  
**NISPOM**—National Industrial Security Program Operating Manual  
**NRO**—National Reconnaissance Office  
**NSA**—National Security Agency  
**ODNI**—Office of the Director, National Intelligence  
**ONCIX**—Office of the National Counter Intelligence Executive  
**OPR**—Office of Primary Responsibility  
**OPSEC**—Operations Security  
**ORCON**—Dissemination and Extraction of Information Controlled by Originator  
**OSD**—Office of the Secretary of Defense  
**PACAF**—Pacific Air Force

**PDS**—Protected Distribution System or Practice Dangerous to Security  
**PED**—Portable Electronic Devices  
**Perm-Cert**—Permanent Certification  
**PFS**—Personal Financial Statement  
**PKI**—Public Key Infrastructure  
**PL**—Protection Level  
**PLA**—Plain Language Address  
**PM**—Program Manager  
**POC**—Point of Contact  
**PPR**—Phased Periodic Reinvestigation  
**PR**—Periodic Reinvestigation  
**PROPIN**—Caution-Proprietary Information Involved  
**PWS**—Performance of Work Statement  
**RFS**—Request for Service  
**RI**—Routing Indicator  
**SAB**—Scientific Advisory Board  
**SAC**—Special Agreement Check  
**SAF/AA**—Administrative Assistant to the Secretary of the Air Force  
**SAF/AAZ**—Administrative Assistant to the Secretary of the Air Force Security, Special Program Oversight and Information Protection  
**SAP**—Special Access Program  
**SAV**—Staff Assistance Visit  
**SCE**—Service Cryptologic Element  
**SCESG**—Scattered Castles Executive Steering Group  
**SCI**—Sensitive Compartmented Information  
**SCIF**—Sensitive Compartmented Information Facility  
**SecAF**—Secretary of the Air Force  
**SES**—Senior Executive Service  
**SETA**—Security Education Training and Awareness  
**SF**—Standard Form  
**SIF**—Security Information File  
**SIGINT**—Signals Intelligence  
**SIO**—Senior Intelligence Officer

**SIPRNET**—Secure Internet Protocol Network  
**SMO**—Security Management Office  
**SOP**—Standard Operating Procedure  
**SOW**—Statement of Work  
**SPA**—Special Purpose Access  
**SPP**—Standard Practices & Procedures  
**SSA**—Special Security Agreement  
**SSD**—Special Security Directorate  
**SSN**—Social Security Account Number  
**SSBI**—Single Scope Background Investigation  
**SSBI-PR**—Single Scope Background Investigation Periodic Reinvestigation  
**SSO**—Special Security Officer/Office  
**SSR**—Special Security Representative  
**STC**—sound transmission class  
**SVA**—Secure Vault Area  
**TCC**—Telecommunications Centers  
**TCO**—TK Control Officer  
**TIS**—Transfer-in-Status  
**T-SCIF**—Tactical Sensitive Compartmented Information Facility  
**TSCM**—Technical Surveillance Countermeasures  
**TSWA**—Temporary Secure Working Area  
**US**—United States  
**USAF**—United States Air Force  
**USAFE**—United States Air Force Europe  
**VTC**—Video Teleconference  
**WBT**—Web-Based Training

### *Terms*

**Access**—Specific type of interaction between a subject (i.e., person, process, or input device) and an object (i.e., a computer resource such as a record, file, program, output device) that results in the flow of information from one to the other. Also, the ability and opportunity to obtain knowledge of classified, sensitive unclassified or unclassified information.

**Access Authorization**—Formal act required to certify that an individual who has been determined to be eligible is authorized to have access to classified defense information; for example, SCI and/or collateral.

**Access Certification**—Temporarily certifies individual access to another organization/ SCI facility for a specific time to accomplish a task (meeting), conference, seminar, etc.

**Access Suspension**—Temporarily withdrawing access to classified information due to a circumstance or incident which has a bearing on eligibility for access to classified information.

**Accreditation**—Formal declaration by a designated authority that a particular physical facility, information processing system, or communications system meets a minimum security standard for the protection of classified or other sensitive information.

**Adjudication**—Process of determining an individual's eligibility for access to national security information.

**Closed Storage**—Storage of SCI material in approved GSA security containers within a SCIF when the SCIF is not occupied by authorized personnel.

**Code Word**—Series of designated words or terms used with a security classification to indicate that the material classified was derived through a sensitive source or method, constitutes a particular type of SCI, and is therefore, accorded limited distribution.

**Cognizance**—Refers to security control, responsibility and jurisdiction of supported units.

**Cognizant Security Authority (CSA)**—Single principal designated by the AF HICE as responsible official for security program management with respect to the protection of intelligence sources and methods. The AF designated CSA is AF/A2ZS.

**Cohabitation**—Arrangement whereby two people decide to live together on a long-term or permanent basis in an emotionally and/or sexually intimate relationship.

**Collateral Information**—All national security information classified CONFIDENTIAL, SECRET, or TOP SECRET under the provisions of an Executive Order for which special IC systems of compartmentation (such as SCI) are not formally established.

**Command Information Systems Officer (CISO)**—Individual responsible to the AO for ensuring that security is provided for and implemented throughout the life cycle of a system or network from the beginning of the concept development phase through its design, development, operation, maintenance, and secure disposal.

**Compartmentation**—Formal systems of restricted access to intelligence activities. Such systems are established to protect the sensitive aspects of specific sources, methods, and analytical procedures of foreign intelligence programs.

**Compartmented Address Book (CAB)**—DIA document which lists the addresses of all SSO and CSSO within the DoD.

**Compelling Need**—Requirement to grant a particular individual access to SCI when that person does not possess the required security clearance or meet personnel security standards. The justification for access shows that the benefits to be gained clearly and substantially outweigh the risks involved, explain why another cleared person cannot perform the task, and explain why the individual cannot be processed normally for SCI access. A compelling need exists when denying access would result in mission failure or serious mission degradation.

**Compromise of SCI**—Loss of control over any SCI resulting in a reasonable assumption that it could have, or confirmation of the fact that it has, become known to unauthorized persons. An

SCI compromise need not be assumed if the unauthorized person can reasonably be expected to maintain absolute secrecy over the SCI to which the person was exposed.

**Compromise Determinations**—Determination made by an SCI security violation inquiry official on the possibility of SCI compromise.

**Compromise Certain**—SCI has irretrievably left SCI control; uncontrolled dissemination can be confirmed.

**Compromise Probable**—SCI has left SCI control; uncontrolled dissemination may reasonably be expected to occur, but a specific threat cannot be identified.

**Compromise Possible**—The possibility of uncontrolled dissemination of SCI cannot be ruled out, but with no specific indication to believe such dissemination takes place.

**Compromise Improbable**—Cases in which uncontrolled SCI dissemination is unlikely but cannot be positively ruled out.

**Compromise None**—Certain that SCI did not leave SCI controls and was not exposed to unauthorized personnel.

**Continuous Operations**—For SCI security purposes, this condition exists when an SCI facility is manned 24 hours a day by appropriately indoctrinated personnel. The individual or individuals occupying the SCIF have a continuous capability of detecting unauthorized entry into the SCIF. Positive identification and access control is maintained at all entrance points not fully secured.

**Contractor**—Individuals employed by a contractor company under contract to a DoD agency, department, or activity. Contractor personnel are authorized compartmented access only for the duration of a particular contract.

**Contracting Officer's Representative (COR)**—Indoctrinated personnel (military or civilian) appointed by the Contracting Officer to monitor the day-to-day activities of DoD SCI contracts or serve as a technical representative. They serve as a POC for FSO/CSSO/SSOs as required.

**Contractor Special Security Officer (CSSO)**—Security officer at the contract location (where the work is being done for the contract). The CSSO is responsible for the security of the Contractor Special Security Office (also abbreviated as "CSSO"). Reports through the supporting SSO and contract monitor to the AF CSA.

**Courier**—An AD military person (including reservists or National Guardsmen on AD), DoD civilian or DoD contractor/consultant who hand carries classified information or material.

**Co-Utilization Agreement (CUA)**—Written agreement between two organizations wherein the organization with cognizant ownership of an SCI Facility agrees to the co-utilization of the SCIF by another organization. CUA clearly specify SCIF security requirements and the operational responsibilities to be fulfilled by the parties to the agreement. Organizations that petition to co-utilize a SCIF need to have a clearly defined intelligence mission requiring ongoing handling, review, and dissemination of SCI or similar highly sensitive material for which the protective environment of a SCIF is essential.

**Covered Employment**—Direct employment by, representation of, or the provision of advice relating to national security to the government of a foreign country or any person whose

activities are directly or indirectly supervised, directed, controlled, financed, or subsidized, in whole or in major part, by any government of a foreign country.

**Covered Positions**—A position within the AF element of the Intelligence Community that allows access to Top Secret Sensitive Compartmented Information (TS/SCI)

**Date-Time-Group (DTG)**—Electronic message identifier entered by the proper releasing authority (i.e., 261445Z MAR 90).

**DD Form 254, DoD Contract Security Classification Specifications**—Provides guidance to both the contractor and the government. It is a legal document that directs the contractor as to the proper protection of classified material released under the contract.

**Debriefing**—Process of informing a person that: His or her need-to-know for access to SCI has been terminated. He or she continues to be bound by all security directives and public law pertaining to the security of SCI unless released from that obligation by a competent authority. He or she is required to subscribe to and fulfill a termination acknowledgment.

**Declassification**—Removal of official information from the protected status afforded by security classification; it requires a determination that disclosure no longer would be detrimental to national security.

**Defense Courier Division (TCJ3-C, USTRANSCOM)**—Organization which provides for the secure and expeditious transportation and delivery of qualified material which requires handling by courier. It is the primary means of transferring bulky or large SCI documents/material (Formerly Defense Courier Service).

**Disclosure**—Showing or revealing classified intelligence, whether orally, in writing or any other medium, without providing the recipient with a copy of such information for retention.

**DoDIIS Site**—The DoDIIS Site-Based Authorization Process uses management techniques to assess risk by establishing a security domain called a “DoDIIS Site”. This concept incorporates Site Security Management as a function of the DoDIIS Site’s CM process. A DoDIIS Site Security Baseline defining the systems infrastructure is required and any changes to the baseline is documented in a timely manner. Before a DoDIIS site can establish a Site Security Baseline and be accredited, all system(s) go through the security A&A process. The Site Security Baseline begins with the evaluation and authorization of all individual ISs at the site. All ISs are then consolidated into this single management entity and evaluated as part of the security environment in which they operate. Site-Based Authorization ex The maturity of site security policies, procedures, configuration management, system integration management, and risk management determines the site’s ability to successfully establish and control a secure baseline."

**Due Process**—Due process has three elements, all of which apply when adverse actions with respect to SCI access determination are proposed. Individuals must: 1) Be provided notice of the proposed adverse action; 2) Be given an opportunity to respond to the decision maker proposing the adverse action; and, 3) Be afforded the right to appeal a final adverse decision.

**Eligibility**—Adjudicative determination that an individual meets all the requisite requirements for access to classified information.

**Emergency Action Plan (EAP)**—Plan to be used during natural disasters, hostilities, or other emergencies. Stresses the importance of personnel safety; provides for the safeguarding of SCI, when possible, and the evacuation or destruction of SCI, when necessary; identifies items to be

destroyed in their order of priority. The EAP includes procedures for conducting exercises, orientations and inspections.

**Formal Access Approval**—Documented approval to allow access to a particular category (or classification level) of information.

**Government of a Foreign Country**—Any person or group of persons exercising sovereign de facto or de jure political jurisdiction over any country, other than the US, or over any part of such country, and includes any subdivision of any such group and any group or agency to which such sovereign de facto or de jure authority or functions are directly or indirectly delegated. Such term includes any faction or body of insurgents within a country assuming to exercise governmental authority whether such faction or body of insurgents has or has not been recognized by the US.

**Head of the Air Force Element of the Intelligence Community**—Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance, AF/A2 is the Head of the AF Element of the IC (AF HICE). Heads of the IC are the leads of departments and agencies within the IC, or their designated representatives.

**HUMINT Special Control Officer**—Individual responsible for managing the HUMINT Control System security program and for the security and control of HCS protected information within their organization. Sometimes also referred to as the HCS Control Officer or HCS SSO.

**Immediate Family**—Consists of the individual's spouse, parents (or stepparent when a close and continuing relationship exists), brothers, sisters, children, father/mother-in-law, grandparents, and cohabitants.

**Indoctrination**—Initial instruction and indoctrination acknowledgment before granting an individual access to SCI which concerns the unique nature of SCI, its unusual sensitivity, and the special security regulations and practices for its handling.

**Intelligence Community**—The intelligence community includes the following organizations: Air Force (A2); Army (G2); Coast Guard (Department of Homeland Security); Marine Corps (N2); Navy (N2); Central Intelligence Agency; Defense Intelligence Agency; Department of Energy (Office of Intelligence and Counterintelligence); Department of Homeland Security (Office of Intelligence and Analysis); Department of State; Department of Treasury (Office of Intelligence and Analysis); Drug Enforcement Administration (Office of Intelligence and Analysis); Federal Bureau of Investigation (National Security Intelligence); National Security Agency; National Geospatial-Intelligence Agency; National Reconnaissance Office.

**Intelligence Information**—Intelligence information and related materials include the following information, whether written or in any other medium, classified pursuant to E.O. 13526 or any predecessor or successor Executive Order: 1) Foreign intelligence and counterintelligence defined in the National Security Act of 1947, as amended and in Executive Order 12333, 2) Information describing US foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodology used for the acquisition, processing, or exploitation and the results of the exploitation; and any other data resulting from US intelligence collection efforts; and, 3) Information on Intelligence Community protective security programs (e.g., personnel, physical, technical, and information security).

**National Intelligence**—Integrated departmental intelligence that covers the broad aspects of national policy and national security, is of concern to more than one department or agency, and transcends the exclusive competence of a single department or agency.

**National Intelligence Estimate**—Strategic estimate of the capabilities, vulnerabilities, and probable courses of action of foreign nations which is produced at the national level as a composite of the views of the intelligence community.

**Need-to-Know**—Determination by an authorized holder of classified information that access to specific intelligence in his/her possession is required by another person to perform a specific and authorized function to carry out a national security task.

**Non-Disclosure Statement (NdS)**—Written agreement (DD 1847-1), signed by a candidate for SCI access, promising not to disclose the SCI information they have access to, to unauthorized individuals.

**ODANS**—DSSCS Address Group (DAG) used by CSA to disseminate intelligence security policy for SCI security.

**Owning SSO**—SSO responsible for SCI cognizance of individuals, facilities and systems within their chain of command.

**Open Storage**—Maintenance of SCI material within a SCIF in any configuration other than within GSA-approved security containers, while such SCIF is not occupied by authorized personnel.

**Perm-Cert**—Permanent certification for SCI access. Certifies an individual for a specific period of time. Requires at least annual renewal. Used for persons whose SCI personnel security accountability is held by another command or IC department/agency.

**Personal Data**—Information that concerns an individual's habit, conduct, emotional stability, or personal circumstances which may be used to assess his or her eligibility for retention in SCI indoctrinated status.

**Personal Financial Statement (PFS)**—Written statement completed by candidates for SCI access when there are indications of possible financial difficulties.

**Plain Language Address (PLA)**—Plain language address is a phrase used to denote the abbreviated language spelling of an activity short title used in message addressing. DSSCS PLAs are listed in the Compartmented Address Book.

**Re-Indoctrinations**—A process of repeating the SCI indoctrination procedure at a regular interval. Such a repetition may be required for purposes of re-emphasizing SCI security practices or for other appropriate reasons.

**Release**—Providing the recipient of classified information with a copy, whether in writing or any other medium, of such information for retention.

**Resource Management System (RMS)**—Methods and procedures used in the DoD that: (1) deal with resources (manpower, equipment, services, materials, supplies and funds); (2) assists in the management of such resources (planning, budgeting, acquisition, use, consumption, storage, and disposition); and (3) provides for a system of recurring collection of information.

**ROXAD**—DSSCS Address Group (DAG) used by CSA to disseminate security education and awareness information to the field.

**Sanitization**—Concealment of sensitive intelligence sources, methods, and analytical procedures through editing and/or altering of intelligence information. Objective is to permit dissemination of intelligence information outside of compartmented systems.

**Sanitize**—Systematic process of removing or concealing classified information and materials from the view of un-cleared personnel.

**Security Incident**—Security incidents are categorized as either Violations or Infractions.

**Security Violations**—1) Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information. 2) Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of Executive Order 13526 or its implementing directives; or 3) Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of Executive Order 13526.

**Infractions**—Infraction (formerly known as Practice Dangerous to Security) is a failure to comply with the provisions of security regulations or this manual or any other action that causes a potential compromise of classified information.

**Security Information File (SIF)**—File consisting of documents collected pursuant to making a determination concerning an individual's continuing eligibility for access to classified information. A SIF on any SCI-indoctrinated person is maintained by the servicing SSO and not the base Information Protection Office.

**Secure Vault Area (SVA)**—SCIF under the security jurisdiction of the designated SVA Custodian. It is identical in operation to an SSO except that it normally has no internal SCI communications capability.

**Secure Working Area**—Accredited facility used for handling, discussing, and/or processing of SCI but where SCI is not be stored.

**Senior Intelligence Officer (SIO)**—Highest ranking individual who is charged with direct foreign intelligence missions/functions/responsibilities within a component, command, or element of an IC organization. If an organization has no (or a limited) intelligence mission or function, but requires SCI, the commander designates an officer as the SIO for SCI purposes.

**Sensitive Compartmented Information (SCI)**—Information and materials requiring special community controls indicating restricted handling within present and future community intelligence collection programs and their end products. SCI was established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs. The term does not include Restricted Data as defined in Section II, Public Law 585, Atomic Energy Act of 1954, as amended.

**Sensitive Compartmented Information Facility (SCIF)**—Accredited area, room, group of rooms, or installation where SCI may be stored, used discussed and/or electronically processed. SCIF procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF.

**Service Cryptologic Element (SCE)**—Term used to designate separately or together those elements of the US Army, Navy, and AF which perform cryptologic functions; Navy and AF elements are also known as Service Cryptologic Agencies (SCA).

**Sharing**—Activities involving the disclosure or release of intelligence.

**Signals Intelligence (SIGINT)**—SIGINT is intelligence information which comprises COMINT and ELINT as those terms are defined herein. In addition, and for the purposes of this publication, SIGINT includes foreign instrumentation signals (e.g., telemetry and beaconry).

**Special Access Program (SAP)**—A program established to control access, distribution, and provide protection for particularly sensitive information beyond that normally required for TOP SECRET, SECRET or CONFIDENTIAL information—A Special Access Program can be created or continued only as authorized by a senior agency official delegated such authority pursuant to Executive Order 13526. (NISPOM)

**Special Security Officer (SSO)**—System through which the Director, DIA; the Army, Navy, and AF Intelligence Chief; and AF supported Unified and Specified Commands perform their responsibilities for the security, use, and dissemination of SCI. The symbol SSO is used to refer to the office, the officer and the staff.

**Servicing SSO**—SSO providing administrative support for all individuals external to their chain of command as requested by an owning SSO.

**Special Security Representative (SSR)**—Person responsible for the day-to-day management and implementation of SCI security and administrative instructions for a separate subordinate SCIF.

**Sub-compartment**—Breakdown of a compartment, such as TK, which uses a program based on certain sources, and dedicated to a particular mission and area of interest.

**Technical Material**—Data concerning foreign cryptographic systems; foreign communications systems, procedures, methods, and activities; and methods and equipment designed for COMINT activities.

**Technical Surveillance Countermeasures (TSCM) Survey**—Thorough physical, electronic, and visual examination by special agents from AFOSI or similar DoD agencies in and about an area to detect technical surveillance devices, technical security hazards, and attempts at clandestine penetration of the facility for hostile technical collection of classified and sensitive information. TSCM surveys differ from TEMPEST surveys in that the latter are limited to investigation and studies of compromising emanations whereas the TSCM surveys are basically designated to prevent the technical penetration efforts of a hostile intelligence service.

**Telecommunications**—For the purpose of this manual, a general term expressing data transmission between computing systems and remotely located devices via a unit that performs the necessary format conversion and controls the rate of transmission.

**Telecommunications Center (TCC)**—Communications center may be a dedicated DSSCS, DSSCS/GENSER, or GENSER only communications center.

**Temporary Eligibility**—When access to SCI is justified by the Commander/Director prior to completion of requisite investigation. Eligibility is based on favorable screening interview and

AF CAF approval. Continuing access is contingent upon favorable adjudication of completed background investigation.

**Temporary Secure Working Area (TSWA)**—Area, room, or group of rooms (for example, briefing rooms, conference rooms, ADP areas) which have been properly secured against physical and audio penetration for the temporary (not to exceed an average total of 40 hours a month within a 12-month period) use of SCI. No storage of SCI is permitted in a TSWA.

**TK Control Officer (TCO)**—On behalf of the commander, the TCO inspects local TK facilities and for the security control, use and dissemination of TK material and related security education programs. Tenant units will also be inspected when requested by those commanders.

**Transfer-in-Status (TIS)**—TIS allows an SCI-indoctrinated person to transfer from one assignment to another with no interruption in their SCI-indoctrination. It is the responsibility of the gaining SSO to request a TIS from the losing SSO.

**Attachment 2**  
**SCI SCREENING INTERVIEW**

(FOUO when filled-in)

\_\_\_\_\_  
(Name, Grade and SSN of Interviewee)

1. The purpose of this interview is to assist in determining the acceptability of an individual for nomination and further processing for a position requiring access to Sensitive Compartmented Information (SCI). It is prescribed by DoDM 5105.21, "SCI Administrative Security Manual", DoD Regulation 5200.2R, "DoD Personnel Security Program", and AFI 31-501, "Personnel Security Program Management."
2. SCI screening interviews are conducted when there is no current investigative information available to make an adjudicative determination of eligibility for access to SCI or the interviewee has been out of access for more than 60 days. This interview is voluntary and may be terminated at any time.
3. Any information developed during this interview is made available only to those authorities involved in processing your nomination, those conducting the SSBI, and those adjudicating your investigation for an eligibility determination, or as otherwise authorized by Executive Order or Statute.
4. Penalties for Inaccurate or False Statements. The US Criminal Code (title 18, section 1001) provides that knowingly falsifying or concealing a material fact is a felony which may result in fines and/or up to 5 years of imprisonment. In addition, Federal agencies generally fire, do not grant a security clearance to, or disqualify individuals who have materially and deliberately falsified these forms, and this remains a part of the permanent record for future placements. Answer all questions truthfully and completely. You have adequate opportunity to explain any information you give to us on this form and to make your comments part of the record.

\_\_\_\_\_  
(Signature of Interviewer)  
(Complete Name and Grade)  
(Position) (Organization Designation)

\_\_\_\_\_  
(Date)

I understand the purpose of this SCI Screening interview and elect to proceed/decline.

\_\_\_\_\_  
(Signature of Interviewee)

\_\_\_\_\_  
(Date)

Page 1 of 3

Initials \_\_\_\_\_

INTERVIEWEE INITIALS and DATE: \_\_\_\_\_

<b>All yes answers require a full narrative explanation. Please understand if you decline to provide such explanation, this may slow the adjudicative process and delay your access to SCI.</b>	<b>Yes</b>	<b>No</b>
1. Has your marital status changed since you completed your SF 86/eEquip package; have your married, divorced, or begun cohabitating?		

2. Are any members of your immediate family NOT US citizens? (Immediate family members consist of the individual's spouse, parents [or stepparent when a close and continuing relationship exists], brothers, sisters, children, father/mother-in-law, grandparents, and co-habitants.)		
3. Do you are anyone in your immediate family claim a dual citizenship with another country?		
4. Have you visited any foreign countries since you completed your SF 86/eQuip package? If so, please provide the dates, the countries visited and the reason for the visit.		
5. Have you consulted with a mental health professional since you completed your SF 86/eQuip package? Was this court ordered or based on violence on the member's part? If yes, please explain.		
6. Have you been arrested since your last investigation? If yes, please explain.		
7. Have you ever had any adverse involvement with alcohol (e.g., DUI, alcohol treatment, drunk in public, accident where alcohol was a factor)? If yes, please explain.		
8. Have you used illegal drugs or illicit substances since you completed your last SF 86/eQuip package? If yes, please explain.		
9. Have you had a clearance suspended, denied, or revoked since your last investigation or in the last seven years? If yes, please explain.		
10. Have you had any bills referred to a collection agency since you last completed an SF 86/eQuip package? If yes, please explain.		
11. Have your wages been garnished, have you had any vehicles repossessed, have any tax liens been placed against you, or have you filed bankruptcy? If yes, please explain.		

Page 2 of 3

Initials \_\_\_\_\_

**All YES answers from page 2 must be explained in detail.**

Attach additional sheets as necessary.

Additional Comments:

---



---



---



---



---



---



---



---

I have answered all questions to the best of my knowledge and belief. I have not intentionally provided any incorrect or misleading information.

---

(Signature and SSN of Nominee)

NOTICE: The Privacy Act, 5 USC 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Orders 9397 and 13478. Your SSN will be used to identify you for access to Sensitive Compartment Information (SCI). Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certification or determination, or possibly result in the denial of your being granted access to SCI. Executive Orders 10450, "Security Requirements for Government Employees"; 13526, "Classified National Security Information"; and 12968, "Access to Classified Information" are the authorities for soliciting information during this interview.

I have personally interviewed the nominee and have witnessed the signatures in the record of interview.

The nominee:

\_\_\_\_\_ Is nominated for access to SCI.

\_\_\_\_\_ Is not nominated for access to SCI.

Page 3 of 3

Initials \_\_\_\_\_

## Attachment 3

**CERTAIN POST-GOVERNMENT EMPLOYMENT BY HOLDERS OF SCI ACCESS****REQUIREMENT TO REPORT CERTAIN POST-GOVERNMENT EMPLOYMENT BY  
HOLDERS OF SCI ACCESS**

1. NAME (last, first, MI), GRADE, UNIT

---

1.1. I have SCI access.

1.2. I fit one or more of the following categories

Awarded a 14N and 1N Air Force Specialty Code (military);

Assigned to a 0132- job series (civilians);

Assigned to a Defense Civilian Intelligence Professional System (GG-), Defense Intelligence Senior Executive Service (DISES), or Defense Intelligence Senior Leader (DISL) billet (civilians);

Assigned to an Air Force Intelligence, Surveillance, or Reconnaissance organization, including detailees from other agencies; or,

Assigned to AFOSI.

3. (FOUO) Per 50 U.S.C. 3073a, I agree to report to the AF/A2 Cognizant Security Authority any direct employment by, representation of, or the provision of advice relating to national security to the government of a foreign country or any person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized, in whole or in major part, by any government of a foreign country. This requirement begins on the date on which I cease to be authorized access to Sensitive Compartmented Information (SCI) and ends two years later. I agree to make this report upon accepting such employment; and annually thereafter.

4. AF/A2 CSA reporting number is \_\_\_\_\_ and the email address is \_\_\_\_\_ . I understand that I can request a copy of this letter from the Special Security Officer.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

Privacy Act Information: The information in this form is FOR OFFICIAL USE ONLY. Protect IAW the Privacy Act of 1974.